NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

QUALIA: A PRESCRIPTION FOR DEVELOPING A QUALITY HEALTH THREAT ASSESSMENT

by

Beverly A. Pritchett

December 2008

Thesis Advisor:	Robert Simeral
Thesis Co-Advisor:	Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Qualia: A Prescription for Developing a Quality Health Threat Assessment			**5. FUNDING NUMBERS**
6. AUTHOR(S) Beverly A. Pritchett			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The 9/11 Commission Report called for consolidation of intelligence assets in order to unify the knowledge base of the intelligence community agencies. This concept gave rise to the fusion center as a place for the fusion of multiple information sources from local, state, and federal levels of government. Although the need for inclusion of health and medical information in fusion centers has been documented, relatively few have done so, and a product designed specifically toward health and medical intelligence currently does not exist at the state and local level. The purpose of this paper is to document a methodology for development of a health threat assessment as a means for the intelligence community to maintain a decision advantage, particularly at the state and local level where the intelligence developed will provide the most benefit to first responders and the local community. This model demonstrates the need for the public health and medical community to improve collaboration across sectors to produce a more integrated product that enhances the understanding of the entire community, thus developing qualia. This can only be accomplished through trust, complete transparency, and clarification of expectations in order to establish the consummate information sharing community.

14. SUBJECT TERMS Public Health, Intelligence, Fusion, Situational Awareness, Qualia, Threat Assessment, Medical, Social Networks, Collaboration			**15. NUMBER OF PAGES** 125
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

QUALIA: A PRESCRIPTION FOR DEVELOPING A QUALITY HEALTH THREAT ASSESSMENT

Beverly A. Pritchett
Senior Deputy Director, Health Emergency Preparedness and Response Administration,
District of Columbia Department of Health
B.S., Saint Bonaventure University, 1979
M.H.A., Baylor University, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2008

Author: Beverly A. Pritchett

Approved by: Robert Simeral
Thesis Advisor

Richard Bergin
Thesis Co-Advisor

Harold A. Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The 9/11 Commission Report called for consolidation of intelligence assets in order to unify the knowledge base of the intelligence community agencies. This concept gave rise to the fusion center as a place for the fusion of multiple information sources from local, state, and federal levels of government. Although the need for inclusion of health and medical information in fusion centers has been documented, relatively few have done so, and a product designed specifically toward health and medical intelligence currently does not exist at the state and local level. The purpose of this paper is to document a methodology for development of a health threat assessment as a means for the intelligence community to maintain a decision advantage, particularly at the state and local level where the intelligence developed will provide the most benefit to first responders and the local community. This model demonstrates the need for the public health and medical community to improve collaboration across sectors to produce a more integrated product that enhances the understanding of the entire community, thus developing qualia. This can only be accomplished through trust, complete transparency, and clarification of expectations in order to establish the consummate information sharing community.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

AFIS	Animal Plant Health Inspection Service
AFMIC	Armed Forces Medical Intelligence Center
CBR	Chemical, Biological and Radiological
CDC	Centers for Disease Control and Prevention
CIR	Critical Information Requirements
DC	District of Columbia
DHS	Department of Homeland Security
DOD	Department of Defense
DOH	Department of Health
DOJ	Department of Justice
ED	Emergency Department
EMS	Emergency Medical Services
ER	Emergency Room
EPI-X	Epidemic Information Exchange
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FSIS	Food Safety Inspection Service
HAZMAT	Hazardous Materials
HHS	Department of Health and Human Services
HIS	Healthcare Information System
JCAHO	Joint Commission on the Accreditation of Healthcare Organizations
JWICS	Joint Worldwide Intelligence Communication System
I & A	Intelligence and Analysis

IT	Information Technology
NBIS	National Biosurveillance Integration System
NOC	National Operations Center
OODA	Observe, Orient, Decide, Act
PHIN	Public Health Information Network
TS SCI	Top Secret, Sensitive Compartmented Information
WMATA	Washington Metropolitan Area Transit Authority

ACKNOWLEDGMENTS

The time and effort that went into this thesis was the result of the tremendous support and encouragement from my network of friends and coworkers in the National Capital Region and the Naval Postgraduate School. I truly appreciate the sage advice that so many have given me, but in particular Nitin Natarajan and John Donnelly, who not only have been co-workers, but also good friends and mentors throughout this course of study. In addition, I cannot begin to express my gratitude to Neil Troppman, who turned my thoughts into graphic artistry.

I also owe a substantial thank you to my advisors, Richard Bergin and Robert Simeral, who so patiently waited on a product from me. Both of you are amazing in the level of attention and concern you devote to each student that you accept to advise through the thesis process. I would also like to thank Robert Bach who inspired me to think anew and motivated me to implement strategic leadership principles within my sphere of influence in the District Government.

Lastly, I would like to acknowledge the support of my friends and family. Although you are spread across this great nation of ours, your encouragement was felt continuously. In particular, I would like to thank Sarah Canzano and Lisa Schwenk, my nieces, who often provide me a much-needed reminder of the endless possibilities in life through the optimism of young adulthood. I thoroughly enjoy your infectious enthusiasm and I am incredibly grateful for the assistance you provided me with my pet care responsibilities on so many occasions. In addition, I extend a special thank you to Scott Pickett, a fellow classmate and friend, who is the consummate professional. Your ability to make me laugh made this effort tolerable, but more importantly, your encouragement and support is the reason this thesis is completed.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Suddenly, unexpectedly, I had this incredible revelation.

— Andrew Wiles, on discerning the proof of Fermat's last theorem

A. PROBLEM STATEMENT

Chaos may be one way to describe what happened in our government after the attacks on this country on September 11, 2001. However, the study of chaos theory shows that if the essential aspects of chaos are broken down into their smallest elements, we can find patterns amidst the flurry. A flap of a butterfly's wings may not really be capable of creating a tornado (Lorenz, 1972),[1] but the chaos theory principle of "sensitive dependence on initial conditions," forces us to reevaluate the process by which we develop intelligence. In doing so, we may be able to see patterns not seen before, thereby allowing us to get inside the enemy's decision cycle to prevent the next terrorist attack. In reevaluating our intelligence development process, we were called to think anew. In doing so, some states created intelligence fusion centers. The inception of these centers resulted from dual incentives; the responsibility for major portions of homeland security being pushed down to the state and local level, and dissatisfaction with the threat information that the federal government was providing to the states. As of March 2008, there were 58 fusion centers located in states and large cities (Department of Homeland Security [DHS], n.d.). However, the effectiveness of their products has been the subject of significant debate. Critics speculate that many of the products from these fusion centers are nothing more than newspaper clippings (Brueggemann, 2008, p. 14). A lack of analysis regarding the pertinence of the information to the locality and a failure to include disciplines other than law enforcement is prominent in the criticism. Our

[1] This concept is attributed to Edward Lorenz for a presentation he gave entitled *Predictability: Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?* During a conference of the American Association for the Advancement of Science in Washington, D.C., December 1972.

challenge now is to refine the fusion concept by creating qualia through trust and collaboration in the intelligence development process. This will be discussed further in subsequent chapters.

1. Background

The 9/11 Commission Report called for consolidation of intelligence assets at the national level in order to unify the knowledge base of the intelligence community agencies in a network-based, information-sharing system. The purpose of this system would be to create a synergy of information whose whole is greater than the sum of its parts (National Commission on Terrorist Attacks Upon the United States, 2004, p. 394). Having raised this issue to the forefront of the counterterrorism effort, many local and state law enforcement agencies broadened the scope of their intelligence activities to include federal intelligence information as well as other public and private sector data. This trend gave rise to the fusion center concept as a place for the integration and fusion of multiple sources of information from local, state, and federal levels of government.

The Department of Justice (DOJ) Fusion Center Guidelines (2006, p. 2) define a fusion center as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." In support of state and local agencies taking on this effort, Abbot and Hetzel (2005, p. xix) state,

> The fundamental responsibility of the government is the protection of the lives, health and welfare of its people. Incumbent in this mandate is the responsibility of state and local governments to protect residents not only from criminal and terrorist acts, a responsibility normally associated with law enforcement, but also from naturally occurring threats and disasters. Public health related intelligence can play a critical role in protection from all of these threats.

The need for collaboration between law enforcement and health and medical officials in both deterring and investigating crime has been addressed extensively in the literature. Richards (2002) provides an excellent discussion on this topic.

> Public health officials can respond quickly to an indentified threat and can conduct investigations without the limitations of probable-cause warrants… Information from public health investigations may be used in criminal investigations if two criteria are met. First, the information must be collected and processed with a proper chain of custody so that it can be authenticated by an expert and admitted into evidence…Second, the evidence must be obtained as part of a legitimate public health investigation. For example, food samples taken during an investigation of food poisoning at a picnic could be used in a subsequent criminal trial if the food was found to be intentionally contaminated (Bioterrorism Investigations).

The Congressional Research Service report, *Fusion Centers: Issues and Options for Congress*, holds that stakeholders, such as public health, emergency responders, and the private sector, are crucial to developing an accurate picture of the threat to jurisdictions (Masse, O'Neil, Rollins, 2007, pp. 5-6). In addition, Butler, Cohen, Friedman, Scripp and Watz (2002, p. 1155) stress the significance of coordination between public health and law enforcement in bioterrorism planning.

Dr. Jeffery Runge (2008, Threat Awareness), the Assistant Secretary for Health Affairs in the Department of Homeland Security, emphasized that his office is responsible for the development of biological threat awareness by developing and maintaining intelligence sources. Runge (2008) states in his UASI Keynote Address:

> The Department of Homeland Security is doing a lot in the area of threat awareness. The Office of Health Affairs works closely with the Office of Intelligence and Analysis, who in turn work with the broader Intelligence Community, as well as law enforcement at the state and local levels. The Department is working closely with State Fusion Centers to monitor and integrate threat information – with 58 Centers around the country the Department has provided more than $254 million from FY 2004-2007 to state and local governments to support these Centers. Fusion Centers are critical to our mission of preventing an attack from happening in the first place. Good intelligence information is really the only method we have today to stop a biological attack from happening in the first place (Threat Awareness).

Although the need for inclusion of health and medical information and analysts in fusion centers has been documented, relatively few fusion centers have actually done so. In March 2007, Morrissey (2007) documented that only six fusion centers, three

Terrorism Early Warning Groups (TEWG) and three Joint Terrorism Task Forces (JTTF) had some type of health or medical representation (p. 27). This evidence demonstrates that currently there is a gap in the ability of state, local, and tribal levels of government to protect their emergency responders, law enforcement personnel, and residents from health related threats. The gap derives from a failure to include health information in the fusion process. Even those that do include health data have yet to develop a routine process for development of an integrated health threat assessment based upon relevant health and medical data that is available through health departments, other governmental agencies, and the private sector. This assessment can provide the intelligence necessary to develop appropriate protective actions in either natural disasters or criminal/terrorist incidents.

Despite the amount of effort applied to prevention, however, the possibility exists that a terrorist attack may still occur. When this happens, the health sector can also play a critical role, whether the event is an overt attack, such as the 1995 sarin attack in the Tokyo subway, or a covert attack, such as the 2001 anthrax attacks in Washington, D.C. In overt attacks, the input from public health usually is evident in the mitigation mode during emergency response after detection of the incident. In the covert mode, public health epidemiological surveillance may be the first method of detection that an attack has occurred. This early response must focus on diagnosis and medical care. The fact that criminal intent was involved may not be evident immediately; therefore, epidemiological investigation is vital to its discovery (Butler et al., 2002, p. 1152). Epidemiological investigations look across jurisdictions for patterns of illness that may give clues regarding the location where the incident occurred. These investigations are also critical in identifying other individuals that my have been exposed during the event, which will mitigate the degree of illness or fatality rate associated with the incident. Whether overt or covert, health threat assessments are critical components in prevention and response for minimizing casualties.

2. Health Threat Assessment

A health threat assessment is an estimate of the possible diseases and/or injuries that could occur through recognition of sentinel events or patterns within data that provide indications of impending harm (Devon & Cornwall Constabulary Glossary, 2008). Like an intelligence threat assessment, the health threat assessment could be one of the building blocks in the prevention of terrorist attacks and the mitigation of casualties after an attack. It can also assist in developing policy and response plans.

The health threat assessment is not a new concept. The Department of Defense commonly uses this process to ensure the protection of service personnel upon deployment to overseas locations. According to the Armed Forces Medical Intelligence Center (AFMIC), Medical Intelligence Tutorial (2000, p. 4), the assessment consists of a variety of factors categorized according to three major categories: infectious disease and environmental health, medical capabilities, and life sciences and technologies. Although all three of these categories are important, the aspect that will have the greatest threat to first responders is the category of infectious disease and environmental health. This category includes types of infectious diseases considered to be of operational importance either because they are diseases that already exist in the region or because terrorists could introduce these types of infectious diseases as weapons. They include zoonotic associated diseases such as anthrax, food, and water-borne diseases such as cholera, respiratory diseases such as Tuberculosis (TB), sexually transmitted and blood-borne diseases such as Hepatitis, vector-borne diseases such as West Nile Fever, as well as other infectious diseases such as Ebola-Marburg viral disease. The second part of this category includes environmental factors that can affect the health of our workforce and residents, such as environmental pollution from contamination of our air, food, water, and soil with toxic substances (AFMIC, 2000, pp. 9-10, 12).

The obstacles to the development of a comprehensive health threat assessment are represented by the complex nature of accessibility of the information systems and the number of possible data sources. Natarajan (2007) listed 25 types of data points that would have an impact on the health threat (pp. 47-48). This data exists in a variety of

formats, which adds to the complexity of the problem. Some information is stored electronically in databases while other information is collected manually on an as-needed basis. Information sources range from local government agencies to federal government agencies to private sector entities. Confounding the usefulness of the information is that no single agency aggregates this information for consolidated analysis. Appendix A depicts this information in table format. Without fusion and analysis, the information lacks credible predictive value.

The large number of sources and types of information at the local, state, and federal levels demonstrates the complexity of the problem and the imperative to develop a health threat assessment at the state and local level. The development of a comprehensive health threat assessment has not become a standard practice within public health across the country; however, to comply with Homeland Security Presidential Directive #8, state and local fusion centers need to commit to this initiative in order to strengthen information sharing and collaboration capabilities. According to the DHS (2005) Capability-Specific Priorities delineated in Interim National Preparedness Goal, 3.2.1., one of the national priorities is to "strengthen information sharing and collaboration capabilities to enable effective prevention, protection, response, and recovery activities" (p. 12). A comprehensive health threat assessment can contribute substantially to those four phases of preparedness.

B. RESEARCH QUESTION

This thesis will address the question: What is a methodology for developing an integrated health threat assessment?

C. SIGNIFICANCE OF RESEARCH

This thesis adds to the national discussion on intelligence issues in state and local fusion centers. Much of the current debate about the fusion centers pertains to the ability to develop intelligence products that have in-depth analysis and provide estimates of the current threat to local jurisdictions. This thesis presents a possible model for the development of a health threat assessment for use by local and state fusion centers as an

element of a comprehensive threat assessment. This discussion adds a new philosophical perspective to intelligence analysis through discussion of the concept of qualia in the fusion process. The outcome of this research advances the discussion on improving our ability to protect our homeland through the inclusion of health and medical data and the philosophical construct of qualia when developing intelligence threat assessments.

D. LITERATURE REVIEW

1. Health Threat Assessment

The literature in the field of health threat assessment is limited but growing. Currently, the literature is almost exclusively restricted to references surrounding military operations. Military documentation uses the terminology "medical threat assessment," which is a commonly used process in the Department of Defense for ensuring the protection of service personnel upon deployment to overseas locations (AFMIC, 2000, p. 4). The combination of these data elements is intended to provide the military medical planner with the intelligence necessary to develop recommendations for immunizations, level of protective clothing and uniforms, and pharmaceutical prophylaxis to achieve the best protection of the deploying force.

Colonel Robert DeFraites (2007), the Preventive Medicine Consultant to The Surgeon General of the United States Army, published an article on medical situational awareness during the COBRA GOLD 2006 Command Post Exercise in Thailand (p. 1071). DeFraites (2007) argues that the resultant positive outcomes from developing medical situational awareness are that

> This information supports effective and timely decision-making. This ensures that (1) health hazards can be anticipated and protective actions taken; (2) personnel exposed to CBRN, occupational, and naturally occurring environmental threats can be located, informed and treated; and (3) operational plans can be appropriately adjusted in a timely fashion, in collaboration with partner organizations, such as coalition forces and nongovernmental organizations. (p. 1072)

Despite the somewhat limited focus from the military perspective, even less has been done to develop a similar health threat assessment for state and local public health officials relative to their development of the same type of protective action recommendations, treatment when necessary, and alteration of plans based upon the existing threat. The current literature, however, contains complementary information in the development of key concepts that give credence to the importance of the development of a health threat assessment. These three other areas of study include the development of intelligence threat assessments, recognition of indicators and warnings, and public health assessments of specific populations for identification of chronic disease or medical conditions.

2. Intelligence Threat Assessment

The literature surrounding threat assessments is expansive and covers topics such as

- National security challenges to the United States in the Annual Threat Assessment of the Director of National Intelligence (McConnell, 2007).
- Models for developing threat assessments for schools such as *A Guide to Managing Threatening Situations and to Creating Safe School Climates* by the U.S. Secret Service and the Department of Education (Fein et al., 2002).
- Air and maritime domain threat assessments from Transportation Security Administration (2004), such as Security Threat Assessment for Aircraft Operators and Heliport Operators and their Employees that Conduct Air Tour Operations in New York City.
- Computer network security, such as Danforth's Models for Threat Assessment in Networks (2006).
- Nuclear and biological terrorism threat assessments, such as the *Bioterrorism and Threat Assessment* (Ackerman and Moran, 2006) published by the Weapons of Mass Destruction Commission, which was sponsored by the United Nations.

Each of these publications is specific to a particular aspect of homeland security, and all could have some impact on the public health of a community; however, none specifically addresses the health aspect of the threat.

3. Indicators and Warnings

Research has also been conducted in the area of indicators and warnings, primarily in the strategic sense. The literature reveals a body of work in the 1970s and 1980s regarding the intelligence community and its ability or failure to interpret threat indications and warnings accurately prior to enemy attacks. Belden (1977) states, "The warning process – whose primary elements are indicators, analysis, decision, and action – is conceptualized in interaction terms and further specified using the notion of actor's decision stairways" (p. 181). More recently, the Department of Homeland Security distinguishes between intelligence and information gathering in the Target Capabilities List published in September 2007. The Information Gathering and Recognition of Indicators and Warnings capability definition states:

> Unlike intelligence collection, information gathering is the continual gathering of only pure, unexamined data, not targeted collection traditionally conducted by the intelligence community or targeted investigations. Recognition of indicators and warnings is the ability to see in this gathered data the potential trends, indicators, and/or warnings of criminal and/or terrorist activities (including planning and surveillance) against U.S. citizens, government entities, critical infrastructure, and/or our allies. (p. 81)

The Department of Homeland Security (2007) also published an Exercise Evaluation Guide on Information Gathering and Recognition of Indicators and Warnings as a part of its Homeland Security Exercise Evaluation Program (HSEEP). This guide provides a listing of homeland security information gathering and recognition tasks and observations evaluators should assess for during an exercise. However, both the target capability and the guide are almost exclusively geared toward law enforcement. Although both documents reference "other appropriate agencies" (DHS, HSEEP, p. 3), they do not provide specific tasks that should be conducted by other types of agencies.

4. Health Risk Assessment

The third area of the literature closely aligned with health threat assessments is that of population health assessments and health risk assessments. These studies are

geared traditionally toward assessing the health needs of a community to prioritize health care and other interventions. Health assessment studies are conducted by cities at the local level, such as the *Community Health Assessment* of Kansas City, Missouri conducted in 2005, the *Health Status Assessment Report 2006* by the Louisville Metro Health Department, and the RAND Report on *Assessing Health and Health Care in the District of Columbia*, published in 2007 (Lurie et al.). These studies provide assessments of the health indicators of particular populations based on chronic disease registries, hospital admission data, and insurance data claims. However, they do not address immediate threats to population health that stems from natural events or nefarious actions.

Due to the absence of literature on health threat assessments at the state and local level, it is evident that there is a gap in the development of threat assessments. The related literature suggests the need for a public health version of a threat assessment based upon indications and warnings. Recognition of these indicators is critical in enabling public health officials to make recommendations regarding actions necessary to protect first responders and the public.

II. METHODOLOGY

> The greatest obstacle to discovery is not ignorance – it is the illusion of knowledge.
>
> — Daniel Boorstin, Librarian of Congress, 1984

A. MULTITIERED APPROACH TO GROUNDED THEORY

The methodology used for this research is based upon grounded theory, which was developed by Glaser and Strauss (1967). This theory assumes the ability of the researcher to discover theory based on data sampling. As such, instead of gathering data to prove a hypothesis, the researcher develops theory through a looping process of analyzing data for ideas that generate further data gathering until a saturation point is reached. The point at which the researcher achieves saturation will vary from study to study, but it is achieved when the data reveals no new information about the particular subject. This methodology is an effective way for social scientists to develop existing theory further (pp. 45-77).

The multitiered methodology used in this study is not universally accepted. Mingers (2001) discusses the concept of combining research methods within the information systems realm. His research documents the fact that although some work specifically documents a pluralist methodology, this occurs rarely. However, when reviewing the actual procedures used by many authors, the combination of methodologies was apparent (p. 246). The argument in favor of using a multitiered approach is that information systems are much more than simply the information technology that provides their basis. In fact, information systems instead reflect the whole of human communication, including factors such as "psychology, economics, sociology, mathematics, linguistics and semiotics," all of which use very different research methods (Mingers, 2001, p. 252). Because of the similarity between information technology systems and intelligence development, this study's methodology is based on a multitiered research approach. This study uses a sequential research design as documented by

Mingers (2001, p. 252). This methodology employs different research techniques in a sequential manner, the first providing information for the second, and then the second feeding information to the third (Mingers, 2001, p. 246).

Due to the complexity of the subject and the limited documentation in the field of this study, the research methodology used was a triangulation approach that combined a survey instrument and interviews. The process of triangulation allows the use of a variety of research methodologies to develop and validate data that may not be obtainable with just one methodology (Oliver-Hoyo and Allen, 2006, pp. 42-47). Triangulation is a data saturation process that involves approaching the data gathering effort from the use of three methodologies when no single method would be sufficient. In this study, triangulation occurred from gathering data through a survey instrument, validation of that data through structured interviews, which were then followed up by less structured interviews that considered the entire information flow process.

The initial research effort was focused on data gathering using a survey and interviews. The purpose of the survey instrument was to ascertain the types of data elements available to public health professionals in the National Capital Region that could provide health specific situational awareness. In addition, the survey was used to determine the format in which the data is collected and stored. An understanding of the types of information technology systems used by the various agencies with health data to collect, store, and analyze data was essential to determining the appropriate information process flow for the development of an integrated health threat assessment. The second step in the survey process was to interview personnel who develop or maintain the data to verify the data elements discovered from the survey.

Once the researcher was satisfied that the data gathering effort was saturated, a model was developed to depict the various data elements involved, the information flow, the fusion process, product development, and finally, the product dissemination.

The final step in this research process was to conduct interviews. The purpose of the interviews was to validate the data source information and the information process flow model for the development of a health threat assessment. Interviews were conducted

using subject matter experts in the field of both homeland security intelligence and public health. This triangulation approach provided validation concerning saturation of the data gathering effort.

B. DATA GATHERING

1. Survey

The survey instrument, designed using the automated survey tool provided by SurveyMonkey, was an electronic questionnaire comprised of a combination of structured and unstructured questions. A copy of the survey is included in Appendix B. The survey's respondents were a variety of public health professionals serving primarily in the federal or state levels of government, who currently collect or process health or medical data listed in Annex A. Examples of these professionals are experts in pre-hospital care, epidemiologists involved in syndromic surveillance, and those involved in animal disease control or vector-borne disease control. In addition, individuals responsible for biological and chemical surveillance programs at both state and federal levels were surveyed as well. Other professionals surveyed were those involved in food inspection, poison control, and air, water, and soil sampling. The surveys were distributed via email. Annex B contains a copy of the SurveyMonkey instrument that was used.

2. Interviews

To enhance saturation of the data, interviews were conducted with individuals who had similar responsibilities. Questions similar to those in the automated survey were used during this interview process; however, the interviewees were provided with a listing of the data sources that had been developed through the survey process, and the questions were generalized to all public health organizations rather than their specific organizations. These interviews were conducted either telephonically or in person. The intent of the interviews was to ensure clarity and normalcy of the information collected

through the survey. Because of the oral nature of the interviews, the survey participants provided more detail during their discussion for the unstructured questions. This helped to provide greater data saturation.

C. MODEL DEVELOPMENT

1. Model Development

Upon completion of the first phase of research, a knowledge flow model was developed demonstrating the types of data available as well as a possible information flow process in the development of a health threat assessment. The model uses four of the five elements documenting the process presented by Zhuge (2002, p. 25), including information accumulation, classification, abstraction, and analogy.

The model was not focused exclusively on the discrete aspects of information flow; rather, it addressed as well the abstract concepts of information fusion. Development of the model was accomplished after conducting a review of the literature on various models in use in intelligence development and decision making. A combination of theory and documented process was used as the basis for the model.

2. Interviews

Upon completion of the model design, interviews were then conducted to ascertain the validity of the process flow. Interview questions and a copy of the model were provided to interviewees in advance of the interview. If the interview was conducted in person, the individual was provided the information at least two hours in advance in hard copy. If the interview was conducted telephonically, the information was provided at least 24 hours in advance via email. Appendix C contains a copy of the interview questions and the model, which were presented to each individual interviewed.

For this portion of the research, nine individuals were interviewed. The background and experience levels of those interviewed included the following:

- Four state level Directors of Public Health Preparedness
- One state level Chief of a Bureau of Epidemiology
- One Battalion Fire Chief responsible for Special Operations
- One Level One Trauma Center Emergency Preparedness Coordinator
- One Critical Infrastructure Program Manager for the Federal Government
- One Biosurveillance Program Director for the Federal Government

All of these individuals are familiar with the intelligence cycle or public health. Probable stakeholders of a health threat assessment were also included in the interview process. Their input was particularly important regarding the usefulness of such a product to the public health intelligence consumer. Interviews were recorded, transcribed, and coded. Using the grounded theory research tenet of adjusting the research effort based on data collected during field interviews and observations, additional questions were added after the first three interviews due to the emphasis placed on two specific areas by the interviewees. These additional questions were developed to gain further information regarding the types of knowledge management architecture and intelligence products. Based upon information gained in the interviews, the model was modified to incorporate new data points and concepts for the information process flow.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FUSION QUALIA

> At the heart of science is an essential tension between two seemingly contradictory attitudes – an openness to new ideas, no matter how bizarre or counterintuitive they may be, and the most ruthless skeptical scrutiny of all ideas, old and new.
>
> — Carl Sagan, *The Demon Haunted World*, 1996

A. INTELLIGENCE AND FUSION

This chapter will present various models for intelligence preparation and the theory of fusion in the development of intelligence. Based upon these basic models and the results of my research, I will present a model for building a health threat assessment for use at the state and local levels.

1. The Intelligence Cycle

Most texts on intelligence include a discussion on the intelligence cycle or the process by which intelligence is produced (Gill and Phythian, 2006, p. 3; Johnson and Wirtz, 2008, p. 49; Lowenthal, 2006, p. 65). The Fusion Center Guidelines published by the Department of Justice (2006) define the intelligence process as "the means of developing raw information into finished intelligence products for use in decision making and formulating policies/actions" (p. 24). The cycle used at the strategic level by the Central Intelligence Agency (2001, Intelligence Cycle) includes the stages:

- Planning and Direction. This is not really a single phase of the process, but rather is seen as the overall management of the process from collection requirements to product dissemination.
- Collection. This stage involves the collection of data and information, which is often termed "raw" intelligence because it has not yet been analyzed.
- Processing and Exploitation. In this stage, the raw intelligence is transformed into something that is useable by intelligence analysts through processes, such as language translation and de-encryption.
- Analysis and Production. In the development of intelligence, this is the stage at which the experience and training of the analyst is of utmost

importance. This stage is the point where raw intelligence becomes finished intelligence through an evaluation of the validity and relevance of the information in relation to the requirements developed in the planning stage. The products that are produced in this stage must be designed to suit the desired audiences.

- Dissemination. This stage is the logical distribution of the finished product and a return to the original stage of Planning and Direction.

Figure 1 depicts the intelligence cycle as described by the Central Intelligence Agency in the *Factbook on Intelligence*.

Figure 1. The Intelligence Cycle. (From: *CIA Factbook on Intelligence*, 2001)

Because there are multiple versions of the intelligence development process in the literature, many with a concept variation worth noting, five other versions are presented in this discussion. The Federal Bureau of Investigation's Intelligence Cycle includes an additional step, *requirements*, which is added prior to *planning and direction* (Carter, 2004, p. 65). However, Lowenthal (2006) alters the cycle further with a seven-step process by incorporating *requirements*, but deleting *planning* and *direction*, and adding the stages of *consumption* and *feedback*. He describes the requirements stage as the point at which policymakers identify policy issues or decisions about which they expect the intelligence products to inform them. The stage of consumption is the reading or receiving of the briefing of the finished intelligence product. Once presented, Lowenthal

asserts that feedback regarding the quality of the product and the format of presentation is critical for analysts to improve their products. Rather than depicting the intelligence cycle in the typical round pattern, he depicts the intelligence development process in a linear model with multiple layers in order to demonstrate continuous feedback (pp. 54-67). Figure 2 depicts the Lowenthal model.

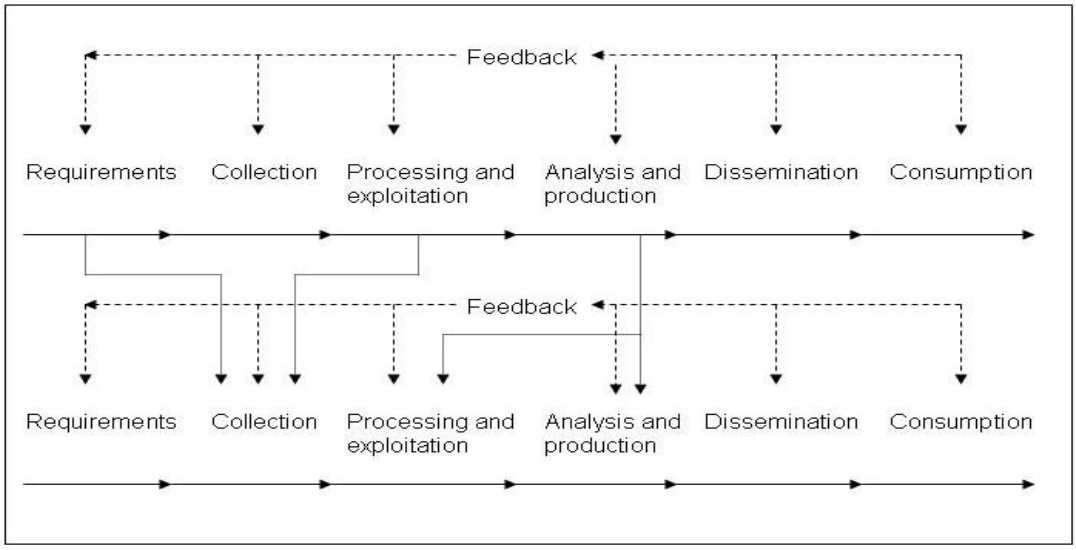


Figure 2. Intelligence Process – Multilayered. (From: Lowenthal, 2006, pp. 54-67)

The Fusion Center Guidelines provide yet another version of the intelligence cycle process with a six-step cycle, which incorporates the five steps of the Central Intelligence Agency's model with the addition of the stage of *reevaluation*. This stage assesses new information to determine whether the analyst can use it to validate existing analysis or to update or improve previous analysis products (DOJ, 2006, p. 20). Figure 3 presents the cycle depicted in the Fusion Center Guidelines.

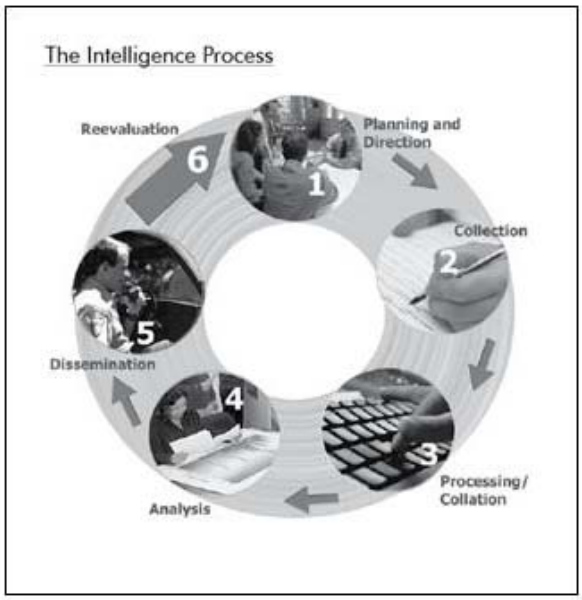


Figure 3. The Intelligence Process from the Fusion Center Guidelines. (From: DOJ, 2006, p. 20).

The variability in the documentation of the intelligence cycle demonstrates the changing nature of the intelligence development process since 2001. The Henry L. Stimson Center documents this change through a comparison of the environmental influences that affect the current development of intelligence. Today's environment involves the need to incorporate sensitive and classified information with volumes of open source information, both of which are available in a variety of formats, including electronic and manually recorded. Another complicating factor is the number of cultures now involved in the intelligence collection and development efforts. The Stimson report discusses the culture of traditional terrorism relative to intelligence development, along with health and natural hazard information cultures (Fisher et al., 2008, p. 5). Table 1 depicts the five-stage process documented by the Central Intelligence Agency, which includes a comparison of the factors that influenced the traditional process with those that mandate an evolution in the process. This comparison documents the increasing complexity in the intelligence development process (Fisher et al., 2008, pp. 7-8).

Intelligence Cycle Stage	Traditional Intelligence Cycle	Evolving Intelligence Cycle
Planning & Direction	Defined consumers; Formal requirements process	Consumers at multiple levels; Conflicting requirements
Collection	Taskings to fill requirements; Resource availability and adequacy understood	Top-down requirements/ bottom-up data; Resource availability
Processing & Exploitation	Technical capabilities embedded within organizations	Technical capabilities dispersed across communities
Analysis & Production	Analytical processes institutionalized and defined	Analytical processes based on different professional expectations
Dissemination	Well-defined products and list of cleared recipients	Varied products with complex security needs

Table 1. Evolving Influences on Intelligence Development. (From: Fisher et al., 2008, pp. 7-8).

Not only does the external environment have a significant effect on the intelligence process, the intelligence process also has an effect on the environment in which it exists. Based upon the concept of the "funnel of causality" first made popular by Campbell, Converse, Miller, Stokes (1980, p. 24), Gill and Phythian (2006) developed a model for the intelligence process that emphasizes the outcomes of the action taken based upon the finished intelligence product. They point out that the funnel shape illustrates that the analysis process filters out a great deal of the raw intelligence data that incorporates the input into the initial process (p. 3). Their model is depicted in Figure 4.

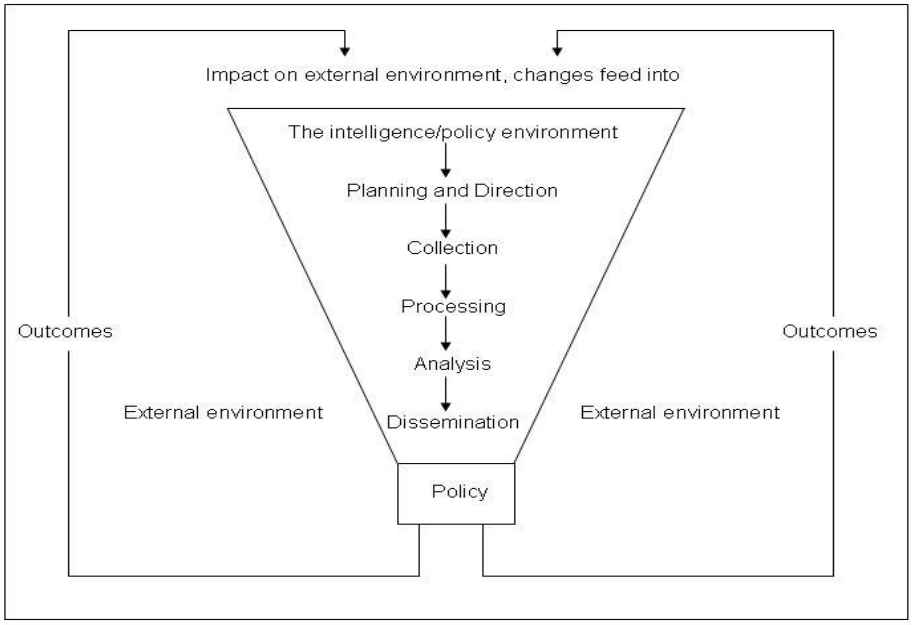


Figure 4. Gill and Phythian Funnel of Causality Intelligence Process (From: Gill and Phythian, 2006, p. 3)

2. The Fusion Process

Based on the number of different models depicting the intelligence process and the variety of factors chosen for emphasis in each model, the complexity involved in this process is evident. The National Governor's Association 2007 survey of homeland security advisors results report that only 56% of the respondents were satisfied with the timeliness of intelligence products and only 50% were satisfied with the "actionability" of such intelligence (p. 6). The fusion process is the stage in the intelligence cycle where raw intelligence and information is turned into actionable knowledge (DOJ, 2006, p. 2). These low statistics seem to verify the complexity of producing quality analysis at the federal level for use by state and local homeland security agencies. However, it may also reflect unrealistic expectations and unfamiliarity with the current capabilities of the intelligence community with consumers at the state and local level.

In a speech by the Director of the Intelligence Staff on November 1, 2008, Burgess (2008) describes the mission of the intelligence community as being to develop a decision advantage over our adversaries in the face of the increasingly complex global situation, which continuously creates new threats.

> We live in a dynamic world in which the pace, scope, and complexity of change are increasing. Increased global connectivity, interdependence and complexity create a less predictable future. Globalization—while it has certainly opened up avenues for growth and prosperity around the world—has also complicated persistent threats and has generated emerging missions, such as cyber, energy, and infectious disease. In addition, changing demographics, population stresses, and resource scarcities have the potential to create economic and political instability worldwide… Our mission in the U.S. Intelligence Community is to create decision advantage through a globally-networked and integrated intelligence enterprise. (p. 2)

Burgess addresses key initiatives in Vision 2015 as being methods to develop such a decision advantage: customer-driven intelligence model, mission-focused operations, net-centric information enterprise, and an integrated enterprise in order to foster collaboration. Successful implementation will be critical to accomplishing that goal. Until then, the ability to provide actionable intelligence to state and local jurisdictions will remain a challenge.

The next part of this discussion will focus on the analysis phase, which is the mainstay of the intelligence process (Lowenthal, 2006, p. 109). The analysis phase consists of two parts, the analysis component and the product development component. This discussion will focus on the analysis component. The critical aspect of the analysis component is the fusion of the various elements of raw intelligence or information. The complexity involved in the fusion process is that combining the data elements is only part of the development of a good analytic product. “Successful intelligence analysis is a holistic process involving both “art” and “science” (Moore and Krizan, 2003, p. 101). Because of the artistry involved, analysis is the part of the intelligence process that is the most difficult to model or document.

The Fusion Center Guidelines define fusion as a supportive process for "implementation of risk-based, information-driven prevention, response and consequence management programs" (DOJ, 2006, p. 11). These guidelines describe the fusion process a method for sharing distributive information from the federal, state, and local levels via a common interface. Figure 5 depicts the fusion process as described above. This figure incorporates the concept that end users can use intelligence products either in a prevention capability when the product is disseminated proactively or in a response capability when the product is disseminated in a reactive or support mode.

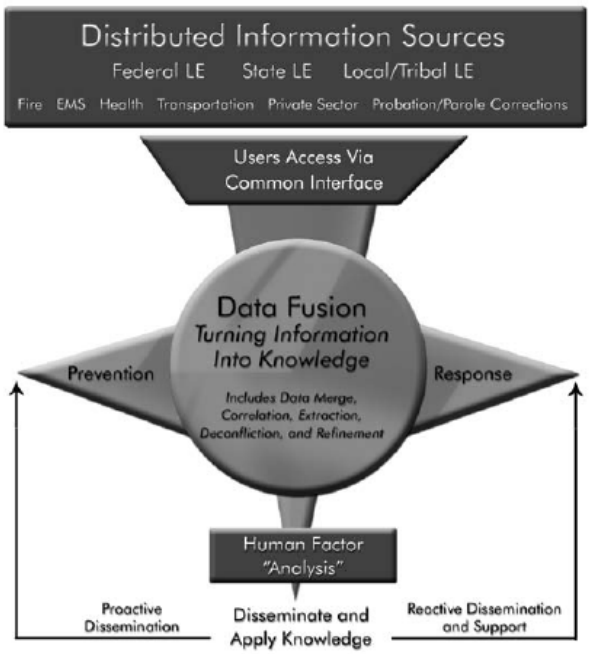


Figure 5. Fusion Process – Fusion Center Guidelines. (From: DOJ, 2006, p. 11).

The guidelines also provide a list of 10 critical elements that must be addressed in order to ensure an effective fusion process, the importance of which has also been noted.

a. Use of Common Terminology

Because of multidisciplinary participation in the analysis process, the potential for misinterpretation of information exists due to the use of the same or similar terms to denote very different concepts. An example is the word *casualty*. In the public

health field, a casualty is an individual who has become ill or injured somehow during an incident. However, in other professions, the term casualty is used when referring to an individual who is deceased.

b. Current Awareness of the Global Threat

In the public health arena, awareness of the global emergence of new zoonotic and other infectious diseases is critical to understanding the potential health threat to the United States because of the ease of global travel and the migratory nature of disease in both animals and humans.

c. Understanding the Linkages between Terrorism and Non-Terrorism Related Information

Again, the health and medical sector plays a significant role in this element. Not all health and medical issues are terrorism related, but almost all terrorism issues have health and medical implications due to the potential for injuries and fatalities. Health and medical information may also play a significant role in responding to terrorist incidents, such as the recognition of a patient's symptoms as being indicative of exposure to a biological agent.

d. Clearly Defined Intelligence Requirements

The definition of intelligence requirements is a challenge for even well seasoned consumers of intelligence. This process must be evolutionary relative to changes in the environment, because as emerging infectious diseases mutate and spread globally, information requirements should reflect those changes. In addition, in order for consumers to establish requirements, they must first understand the changing nature of the potential threat. This requires a meaningful interchange between the analyst and the consumer.

e. Delineation of Roles and Responsibilities of Each Agency

Because of the very nature of fusion, it requires interaction and collaboration between a variety of agencies within different disciplines and from different levels of government. It is imperative that the governance structure address the roles and responsibilities of each agency so that no gaps exist in the review of raw intelligence, and so that each agency understands the limitations of information access and sharing as defined by law.

f. Elimination of Impediments to Information Sharing

The establishment of a collaborative environment is one of the greatest hurdles for members of the intelligence community. At the national level, the intelligence community has developed A-Space, an abbreviation for "Analyst-Space," as a collaborative environment. Time Magazine ranked A-Space among the Year's Best 50 Inventions for 2008. This restricted collaborative environment allows analysts across agency boundaries to discuss ideas about the latest developments in the intelligence arena (Office of the Director of National Intelligence (ODNI), 2008). Within the health and medical community, however, the willingness to share information across agency domains still requires improvement. The Centers for Disease Control and Prevention has an initiative called BioPHusion (Rolka, O'Connor, and Walker, In Press, p. 6), which will integrate many disparate, biologically related data sources. Simultaneously, the Department of Homeland Security is developing its own initiative, known as the National Biosurveillance Integration Center (NBIC) (Eric Myers, Director, National Biosurveillance Integration Center, personal communication, October 15, 2008 at the Health Security Intelligence (HIS) Workshop). Both of these elements intend to have a reporting component to public health practitioners, but the BioPHusion initiative currently produces reports only for "the CDC Director, program leadership and selected external partners" (Rolka et al., p. 6). The NBIC is in its infancy at this point and is not yet developing reports for external partners (Eric Myers, Director, National Biosurveillance Integration Center, personal communication, October 15, 2008 at the Health Security Intelligence (HIS) Workshop).

Several issues affect the ability to share information, including the need by law enforcement to hold close information related to ongoing investigations, the degree of trust that each discipline has with other participating agencies, and the ability for information technology systems to communicate between each other so that information can be shared electronically. Because of years of secrecy about intelligence operations, a new breed of analyst must be developed that encourages information sharing to build a more comprehensive picture of threats in the environment.

g. Interaction with the Private Sector and the Public

Because 85% of our nation's critical infrastructure lies within the private sector, it is imperative that fusion centers and the analysis process include that portion of the private sector at a minimum (Government Accounting Office, 2006, p. 1). One of the most successful endeavors in collaboration between the public and private sectors for the purpose of intelligence fusion is that of the New York City Police Department through its product, known as NYPD SHIELD. The private sector values these reports because they provide timely reports that are accurate, brief, and fact-based (Crosbie, 2008, p. 60).

h. Connectivity with Intelligence and Information Repositories

As mentioned previously under eliminating impediments to information sharing, the ability for analysts to access a variety of information sources is critical for the development of a true and comprehensive understanding of the threat picture. A-Space, BioPHusion, and NBIC all attempt to address this requirement. The greatest limitation to both BioPHusion and NBIC is that their focus is strictly on biological threats. They do not attempt to integrate chemical and radiological information sources, which can also tremendously impact public health (Rolka et al., p. 6); Eric Myers, Director, National Biosurveillance Integration Center, personal communication, October 15, 2008 at the Health Security Intelligence (HIS) Workshop).

i. Participation of Subject-Matter Experts in the Analytic Process

As mentioned in the Stimson report, the complexity and changing nature of analysis and fusion requires that technical capabilities be dispersed across varying disciplines, and that the analysis processes must be geared toward different professional expectations. Because of this, subject matter experts are critical to conducting technically proficient analyses. Many simple solutions exist for incorporating subject matter expertise into the fusion process, including the use of collaborative software, such as Microsoft Groove, Google Applications Sites, and WebEOC. These products will be discussed further in the chapter on knowledge management.

j. Oversight and Accountability to Protect Civil Liberties

Because of the personal nature of a portion of the information collected, the public deserves the right to have that information protected and maintained in accordance with all federal, state, and local laws. This concern is particularly applicable to the health and medical field in the daily collection of health data for syndromic surveillance. Because this information is de-identified at the source, the requirements of the Health Insurance Portability and Accountability Act (HIPAA) are met; however, other identity data elements may be collected upon initiation of an investigation into a disease outbreak, and this information must be protected from disclosure.[2]

These critical elements of the fusion process will be discussed further in the evaluation of the health threat assessment model.

B. JOHN BOYD'S OODA LOOP

1. Decision Making

Colonel John Boyd revolutionized the thought process for United States Air Force pilots when he realized that faster aircraft did not win battles; instead, it was the primacy of the pilots' ability to make quick decisions. Using the same basic concept of developing

[2] The titles of these subparagraphs are summaries of the listing of the issues that must be addressed in order to have an effective fusion process as provided in the Fusion Center Guidelines, pp. 11-12.

a decision advantage in combat, he developed a model called the OODA Loop, which stands for Observe, Orient, Decide, and Act. The approach is based on the simple principle that getting inside the enemy's decision cycle gives you greater advantage than being able to fly or move faster (Curts and Campbell, 2001, p. 4-5). His model, shown in Figure 6, demonstrates the four-phase process of rapid decision making.

This model is easily compared to the stages of the intelligence cycle. In the first stage, the decision maker is presented with multiple inputs, including the sensory events of the unfolding incident and other information, such as input from nearby team members. Upon gathering this information, which is similar to the collection stage of the intelligence cycle, the decision maker processes it against the guidance and control functions implicit in the requirements or planning stage of the intelligence cycle. This information is then pushed forward into the orientation stage in the OODA Loop. In comparing this stage to the intelligence cycle, the orient stage is similar to the analysis stage. Boyd provides greater clarity regarding the various factors that influence the analysis process. He postulates that the individual's cultural traditions, their genetic heritage, and their previous experience interact with new information as it enters the decision cycle during the analysis and synthesis process. While it may seem taboo to include cultural traditions and genetic heritage into the process of decision making, we have seen that radical elements of the Islamic culture use their culture as means to develop a terrorism threat. I would also suggest that cultural traditions could also represent the differing disciplines now involved in the intelligence development process.

Once the information has been processed and the decision maker has determined the implications of the information, the recommendations are fed forward for decision. The decision process is similar to the production stage of the intelligence cycle. Once the decision is made, its dissemination occurs in the process of feeding that decision forward for action, as is the case in the intelligence cycle. Both models contain the feedback loop, which returns information to the assessment of the situation; however, as in the Lowenthal intelligence cycle model, feedback in the OODA Loop enters the decision making process along a continuum rather than being restricted to the beginning of the cyclic process.

The importance of the OODA Loop is that it compares with the intelligence cycle, but it compacts the time into much smaller segments and provides greater clarity regarding the influences on the analyst during the analysis process.

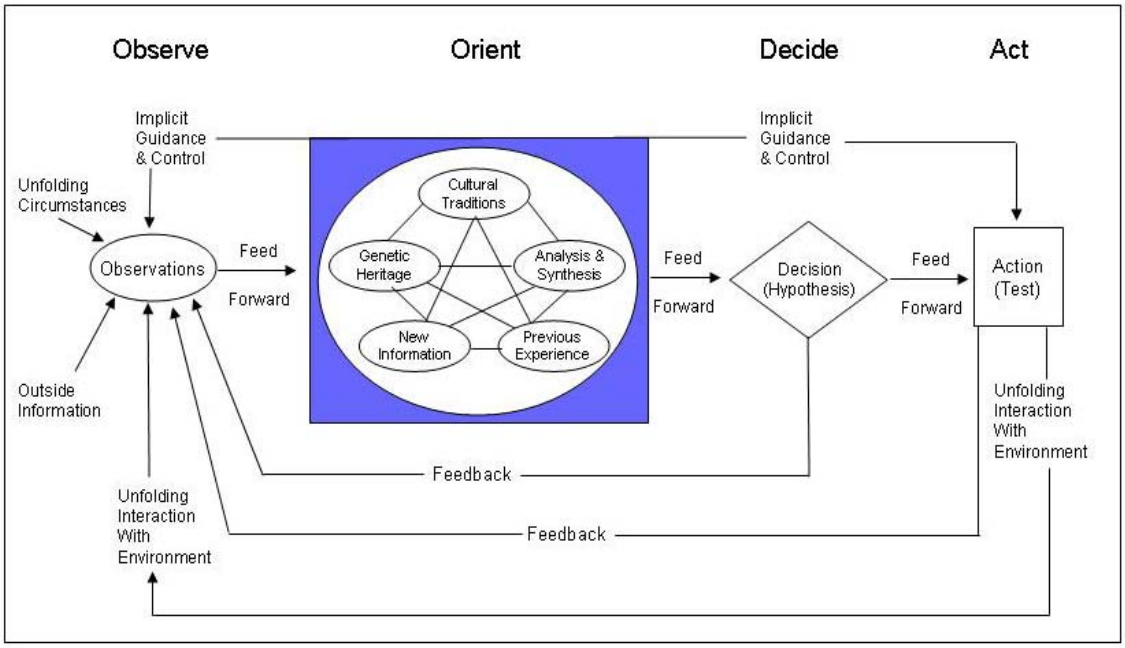


Figure 6. John Boyd's OODA Loop Model. (From: Boyd, August 1987)

C. COGNITIVE HIERARCHY – QUALIA

1. Cognitive Hierarchy

The purpose for the discussion of Boyd's OODA Loop is to demonstrate the varying levels of cognitive hierarchy as one moves through the decision making process. When data points are first encountered, they are discrete, unrelated elements, and they provide us with very little reason to make a decision. As the data points are gathered together, they begin to display some relationship to each other, thus becoming information. The relationship may be categories, such as the number of patients seen with gastrointestinal illness or an usual number of patients with influenza-like symptoms. At this point, we acquire situational awareness, but not necessarily knowledge. In order to

gain knowledge, the information must be analyzed for patterns, trends, and other types of similarities. As knowledge, the cognitive process is incomplete because the actionable element has yet to be formed. This actionable element represents the "so what" factor of the information. What does this information mean to me relative to the situation with which I am involved? This stage of the process involves the cognitive interaction of the individual's training, experience, genetic heritage (according to Boyd), culture, and possibly the insertion of new information. The result of this processing is an understanding of the data. The new understanding is often described as the "aha!" moment.[3]

The concept of the cognitive hierarchy, where knowledge is different from understanding, helps to explain the concept that successful intelligence analysis results from more than the fusion of a collection of multiple data sources. Fusion must provide insights that were not previously known from the individual data elements.

Lowenthal (2006) draws the analogy between intelligence analysis and the assembly of a mosaic. Many pieces are in front of the artist and must be assembled, yet not all the pieces may be present. Some may appear while the mosaic is being assembled, others may get broken so they are no longer the same shape, while still others may become unusable (p. 127). Because of the changing nature of the pieces of the mosaic, the resulting picture is different from the artist's original intent for the design.

Extending the analogy of analysis being an artistic expression, fusion as the basis for the analysis represents the component that enables the assembly of the pieces of information to create a picture or insight that is not otherwise apparent when viewing the individual data points. As new pieces of information are added to the knowledge base, new connections are seen between the new and the old information, thus forming patterns. These patterns establish new insights creating "aha!" moments to form ideas

[3] This cognitive hierarchy was developed from a discussion by Curts and Campbell (2001). I did not agree with all seven levels of the cognitive hierarchy as presented in their discussion, however, and only included the levels that I felt were applicable to this discussion. For further information, see Raymond J. Curts and Douglas E. Campbell, (2001).

that have an impact that is greater than the sum of the data points (Garst and Gross, 2003, p. 105). This moment of comprehending something greater than the analyst had before is the point of reaching true understanding—the *qualia*, as termed by philosophers.

2. Qualia

Qualia—or quale in its singular form—are described as the "introspectively accessible properties of experiences that characterize what it is like to have them" (Tye, 2002, p. 447). More simply, qualia are the phenomenon of experiencing the "what it is like" to have a particular sensation. These sensations can include perceptual experiences, such as seeing a color, hearing a noise, smelling a scent, or touching a texture. Qualia can also refer to bodily sensations, such as feeling faint or pain. The experiences of emotions represent another category considered by philosophers to be qualia, such as love, jealousy, fear, etc. In addition, moods such as depression, boredom, and tension, can also be considered qualia (Tye, 2008).

Jackson (1982) presents the classic discussion of visual qualia. In his example, Mary is a brilliant scientist who knows all there is to know about color. Her training is in neurophysiology, so she knows the physical reaction of the retina when light spectrums enter the eye. Her training includes an understanding of the vocal chords when speaking the words, "red" and "blue." It can be argued that she knows everything there is to know about the physical aspects of color, but she has never seen the color red before. Her life has been restricted to a black and white room, and she can only view the world through a black and white television. The first time she steps outside her room and actually sees red, she experiences something and gains an understanding of the color red that she never had before. Mary acquires a new and phenomenal concept of the color red. That experience is known as qualia (p. 130).

Many philosophers agree that an individual can experience qualia through sight, smell, taste, touch, or sound. However, Strawson (1994) argues that an individual can also "experience" thought. His argument is that the experience of thought results from a complex modification of the quality of one's course of experience that results in the "understanding experience" (pp. 5-10). Therefore, an individual can experience thought

qualia when he or she acquires an understanding of a concept. More importantly, the environment of the situation at the time of the experience influences the experience of understanding a particular concept. Horgan and Tienson (2002) use the phrase phenomenal intentionality to describe the influences made by the environment on the effect of experience (p. 524).

The importance of qualia and phenomenal intentionality to the intelligence cycle is critical to understanding the complexity involved with developing intelligence. When applied to the intelligence cycle and the OODA Loop, qualia can be applied to the concept of the new "understanding" gained during the analysis or orienting process. In this portion of the process, as Boyd and Horgan point out, environmental factors can influence the analysis process. The development of a process for continuous input from the environment will result in an improved intelligence product. The question then becomes how we can develop the process for continuous input from the environment to influence the analysis portion of the intelligence cycle in a positive manner.

3. Health Intelligence Qualia

A scenario that exemplifies the development of health intelligence qualia could be similar to the following:

- A public health analyst sends a report to a public health emergency preparedness official about the theft of several ambulances over the past several weeks in the Midwest portion of the United States.
- The public health emergency preparedness official forwards the report to a local Emergency Medical Services (EMS) agency. EMS personnel read the report and comment that they see the implications to the local area relative to hospitals being soft targets regardless of location, so this could be an area of concern.
- The public health emergency preparedness official replies that not only are hospitals soft targets, but also wonders how many hospitals have the ability to establish alternate emergency room capabilities quickly. In addition, notes that because the city is home to many of the region's level one trauma centers, it is likely that no one would consider an ambulance with license plates from a Midwestern state as being uncommon. This obscurity could result from the large number of ambulances that travel the city daily transporting patients from outlying area hospitals to the trauma centers.

- This exchange of thoughts resulted in a deeper level of understanding (qualia) for both fire and emergency medical services as well as public health emergency preparedness personnel.
- Emergency medical services personnel acknowledge that they will disseminate the information to heighten situational awareness of the potential threat.
- The public health emergency preparedness official instructs the public health intelligence analyst to add this story to the daily fusion center report with the implications as noted above so as to inform local law enforcement personnel to be more aware of ambulances with license plates from external jurisdictions or those with unfamiliar markings. In addition, she also contacts hospitals to ascertain the ability of each to establish alternate emergency room capabilities and discovers that only a few have even the slightest ability to accomplish the task based on current plans. All agree to look into options and report during the next monthly hospital emergency preparedness meeting.
- The completion of this cycle results in an improved understanding of the threat posed to the jurisdiction within multiple first responder categories and allows for implementation of preventive actions and mitigation plans based upon the implications derived through the collaborative discussion.

D. COLLABORATION IMPERATIVE

The scenario described above demonstrates the new understanding that can develop through effective collaboration. As discussed previously, the criteria for development of an effective fusion process found in the Fusion Center Guidelines provides a starting point for examining this concept. A review of those criteria reveals that improving the fusion process implies the construction of an information sharing environment that focuses on collaboration between multiple agencies and experts rather than relying on interpretation of the information by a single analyst. The collaborative environmental factors include development of common terminology, which requires an understanding of the global threat and linkages between terrorism and non-terrorism information through the sharing of information between the national and global communities with state and local health officials. Defining intelligence requirements requires not only a deliberate decision process to focus the analysts' efforts, but it also demands feedback to analysts regarding the utility of their products as well as recommendations for additional areas that require intelligence development based on

changes in the operating environment. The criteria that require the most collaboration from external environmental partners are elimination of impediments to information sharing, interaction with the private sector, participation by subject matter experts, and connectivity with a variety of intelligence streams. These four aspects of intelligence development not only illustrate the need for aggregation of the information streams but also for the need for collaboration between analysts of different agencies and with other external experts.

The literature documents the essential nature of collaboration in relation to intelligence development. McConnell, the Director of National Intelligence said in his Vision 2015 document:

> To transform the [Intelligence] Community and create decision advantage, we will need to accomplish the following … Remove barriers to cross agency collaboration by integrating the strategic enablers of the Intelligence Enterprise – human capital, education and training, business systems, facilities, science and technology, and acquisition and procurement (Introductory Letter)

In a paper published through the Center for Study of Intelligence, Cooper (2005) states:

> The success of the Intelligence Community depends on the promotion of an entire set of effective collaborations: among analysts; between analysts and collectors; between analysts and operations officers; between analysts and the intelligence users; and not least, between community analysts and information sources outside the intelligence or national security enterprise (p. 56).

Collaboration remains a critical element of the intelligence development process, because the need to overcome threats has not diminished since the days of the Cold War; only the nature of the threat has changed (Garst and Gross, 2003, p. 108). The mandate for collaboration within the intelligence community has increased now because of the complexity and technical nature of the information that analysts are expected to review. Subtle nuances in highly technical fields, such as public health and medicine, may only be understood by specific disciplines. Therefore, specific communities of interest will be required to advise on highly technical matters.

E. SUMMARY

This chapter has demonstrated that numerous models describe the intelligence development process, and that a number of individuals have built upon the original model developed by the Central Intelligence Agency. These models have a great deal in common with John Boyd's decision-making OODA Loop. The common element in all of the models is the documentation of the complexity of the analysis process. The basis of the analysis process must be collaboration in order to build the most useful and comprehensive intelligence product. The next chapter will discuss a model for use at the state and local levels for building a specific intelligence product, a health threat assessment.

IV. HEALTH THREAT ASSESSMENT

> Producing machines capable of artificial thought was easy. Producing a machine capable of intelligence has proven elusive because there just isn't anything on which to model it.
>
> — Judge Crater

A. INTRODUCTION

The previous chapter demonstrated the requirement for collaboration in order to produce intelligence qualia. This chapter will present a model for the development of a health threat assessment for use at the state and local levels. This model incorporates the concepts presented in the various intelligence cycle models as well as Boyd's OODA Loop model.

B. FUSION

As discussed in the previous chapter, analysis is the mainstay of the intelligence cycle. The imperative for good analysis is fusion of both the aggregated information sources and the thoughts of analysts, subject matter experts, and operational field personnel. McConnell in his Vision 2015 states:

> By 2015, a globally networked Intelligence Enterprise will be essential to meet the demands for greater forethought and improved strategic agility. The existing agency-centric Intelligence Community must evolve into a true Intelligence Enterprise established on a collaborative foundation of shared services, mission-centric operations, and integrated mission management, all enabled by a smooth flow of people, ideas, and activities across the boundaries of the Intelligence Community agency members. (p. 5)

Because of the importance of information sharing and fusion to the intelligence cycle, this discussion will begin with the focal point of the health threat assessment model, fusion qualia, which is presented in Figure 7.

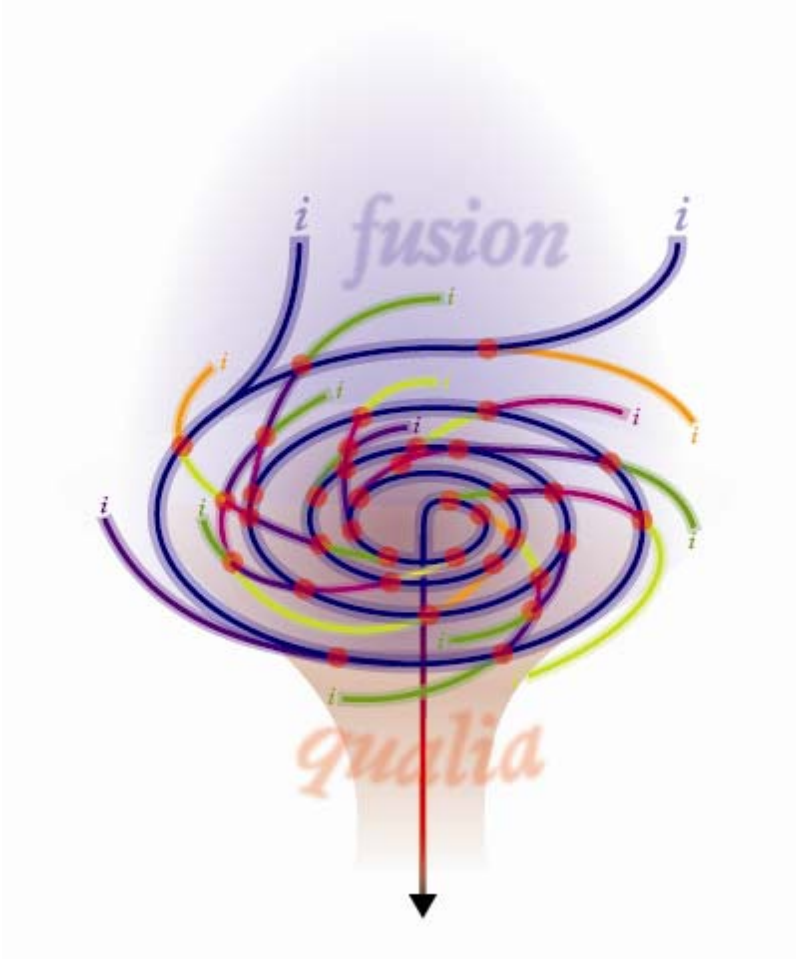


Figure 7. Fusion – Qualia.

This portion of the model, graphically designed by Neil Troppman under direction of the author, demonstrates the aggregation of data or information elements and the fusion of that information as it is reviewed through the analysis process. The multiple colors used on the lines as information enters the process depict different categories of information. This information is either health and medical related information or generic threat information developed by other portions of the analysis process. Examples of the various types of information are syndromic surveillance information, BioWatch daily sampling results, wholesale food distributor inspections, and local threat intelligence. The changing color of the lines after an intersection with another line depicts the addition of some kind of knowledge by combining two pieces of information. It also depicts the exchange of ideas between analysts, thus resulting in increased knowledge. As these lines

continue to intersect various pieces of information with different analysts, a greater understanding of the situation may develop. These points of increased understanding are the intersections noted by the red dots. The red dots represent qualia, the thought process in which this understanding occurs. Qualia are the essential elements of our intelligence development process that must develop in order for the process to be truly effective.

The form of the model is also significant. Reflecting on the funnel of causality referenced in Chapter III, this portion of the model was designed in the shape of a funnel in order to represent the time dimension characteristics of the funnel of causality. Imagine that the central axis represents time and the intersecting lines represent collaborating thoughts and new information passing through time (Campbell et al., 1980, p. 24). As the information is analyzed and lines intersect, some information is culled, new information is formed, and the individual experiences qualia. With each piece of new information is added to the funnel, a better understanding of the threat occurs, and this process continues with some information culled out. This is depicted by the smaller ending of the funnel. Despite the smaller amount of information present, a greater amount of understanding, or qualia, has occurred.

C. HEALTH THREAT ASSESSMENT MODEL

The basis of the model development was derived from the previous models already discussed; the Intelligence Development Cycle using concepts employed in the versions from the CIA Factbook, the Fusion Center Guidelines, and Lowenthal's multilayered process, in conjunction with those in the Funnel of Causality and Boyd's OODA Loop. This model was graphically designed by Neil Troppman under direction of the author.

1. Planning and Direction

The planning and direction portion of the process is an iterative function by leadership that provides priority information requirements for intelligence collection and product development and dissemination guidelines. Although often depicted at the top of

the intelligence cycle, planning and direction can occur at any stage throughout the process. This is shown by aligning it along the entire left side of the health threat assessment model.

2. Collection/Observe

In order to develop the health threat assessment model, the data input selection must be reviewed. Natarajan presented a listing of 25 categories of information that could be collected at the state and local levels for aggregation and analysis. In addition to the listing he presented, I have added other categories that are also available, in Table 2. I have color coded black those presented by Natarajan, while the measures that I have added are color coded in blue. These additional information sources were developed based upon my experience as a Director of Public Health Preparedness for the District of Columbia and were validated or expanded during my survey and interview process. These categories are further classified into information that may be available at the state or local levels and information that is available from the federal government.

Local	Federal
Animal Control	
Radioactive Material Movement/Theft	
Nuclear Plant Operations	
Reportable Disease Surveillance	CDC National Electronic Disease Surveillance System (NEDSS)
Syndromic Surveillance	BioPHusion[4] / BioSense
School Health Disease Surveillance	Epidemic Information Exchange (EPI-X)
Independent Practitioner	
Over-The-Counter Drug Sales	
Pre-hospital Care Diagnosis	CDC Quarantine Stations
Poison Control	National Poisoning Data System

[4] BioPHusion is a combination of 42 different biological related information sources including BioSense, Epi-X, Global Disease Detection-Outbreak Disease Detection Reports, Division of Global Migration and Quarantine Daily Reports, CDC Biosurveillance Coordination Unit, Department of Homeland Security National Biological Information System Reports.

Local	Federal
Long Term Care facilities	
Regional Health Information Systems	
Coroner & Medical Examiner	
Occupational Health	
Laboratory Information System	Laboratory Response Network
Animal Disease Surveillance	
State Department of Agriculture	Animal and Plant Inspection Service, U.S. Department of Agriculture
Carcass Removal	
Behavioral Health	
Food Inspection Retail & Wholesale	
BioWatch	Federal Government Biological Sensors
Private Sector Biological Sensors	Department of Defense Biological Sensors
Soil Sampling Environmental Health	Soil Sampling Environmental Protection Agency
Water Quality Testing	
Air Sampling	

Table 2. Data sets for inclusion in the development of a health threat assessment. (After: Natarajan, 2007)

From the sheer volume of the data presented in Table 2, the complexity of the problem of data aggregation and fusion is obvious. The challenge lies not only in accessing the data but also in gathering sufficient technical expertise to provide interpretation in order for the development of qualia.

Some of these information sources undergo analysis prior to entering the larger fusion process. In many states, epidemiologists electronically collect syndromic surveillance data and analyze the information with automated algorithms. Because this data is not a direct input to the fusion process, the process has been depicted as a separate fusion process and then is input into the larger fusion process in the diagram. The data that may be included in a jurisdiction's syndromic surveillance are hospital emergency

room admission diagnoses, school nurse disease diagnoses, poison control call data, over-the-counter drug purchases, pre-hospital care diagnoses, and regional health information system disease diagnoses from community health centers. In addition, these data points are depicted in separate layers in the diagram to note that some information sources are available at state and local levels and others are strictly available through the Federal government.

3. Processing

This stage prepares raw intelligence data into something that is useable by intelligence analysts. The automated algorithmic processes used to analyze syndromic surveillance data can be viewed as a processing step because the individual data points of each hospital emergency room visit, school nurse illness reporting, etc, would be meaningless unless the instances are compared to trends locally, regionally, and seasonally.

4. Analysis and Production/Orient

The analysis and production portion of the diagram align with Boyd's Orient phase of the OODA Loop. As discussed in the previous chapter, this stage of the intelligence cycle process is the mainstay of the process, and with effective information and thought sharing, qualia can result, thus allowing for the production of a more useful health threat assessment.

5. Decide

The entire intelligence cycle exists to provide actionable information so that decision makers can formulate policies and action. When an analyst attains the level of understanding regarding a particular threat, the decision maker must decide the immediacy of the desired action. Three possible products are:

- Health Threat Alert - urgent information that indicates system action may become necessary at any time. An example might be a suspected norovirus outbreak at a hotel that causes large numbers of visitors to seek health care at a number of local emergency rooms.

- Health Threat Advisory - urgent information but no activation is warranted or expected at this time (i.e., two feet of snow with icy conditions expected tonight. This could lead to a number of accidents resulting in a large increase in casualties being evacuated to hospital emergency rooms). This information is for situational awareness only.
- Health Threat Update - non-urgent information, but sufficiently important to update information that has already been disseminated. An example of this would be confirmation by the public health laboratory that the foodborne illness was determined to be norovirus.[5]

6. Act / Disseminate

The final stage of the health threat assessment process is dissemination of the intelligence with guidance on actions to take. The dissemination process can occur through a multitude of technologies, including the Health Alert Network (HAN), email, WebEOC, or other information sharing technologies.

The actions recommended may be specific personal protective measures, such as reminders to use universal precautions, pharmaceutical prophylaxis, and treatment protocols, advisories to review decontamination and treatment for specific chemical agents, and requests for acquisition of specific specimen types; i.e., blood, fecal, or vomitus.

7. Feedback

It is extremely important that analysts and information sources receive feedback on the usefulness of the products and the information provided by the various sources. This is imperative for the process to improve continually and thus produce products that meet the needs of the consumers and stakeholders. In Vision 2015, McConnell states:

> Old problems assume new dimensions: information operations with emphasis on a cyber domain, asymmetric political or military responses, and illicit trafficking. Lastly, we confront the challenge of acting in an environment that is more time-sensitive and open to the flow of information, in which intelligence sources and analysis compete in a

[5] These alert levels are consistent with those established by the Centers for Disease Control and Prevention per their "Guidance for Developing Public Health Alerts, Advisories, or Updates."

> public context established by a global media. By 2015 we will need integrated and collaborative capabilities that can anticipate and rapidly respond to a wide array of threats and risks. (p. 5)

,This model of a health threat assessment presents documentation of a process for addressing the problem of disconnected information sources across a state or local jurisdiction in conjunction with information sources within the Federal government. The model demonstrates the ability to integrate and collaborate in order to build a health threat assessment through fusion qualia to respond to a wide array of health and medical threats.

Figure 8 depicts the health threat assessment process and its relationships with the traditional Intelligence Cycle and Boyd's OODA Loop.

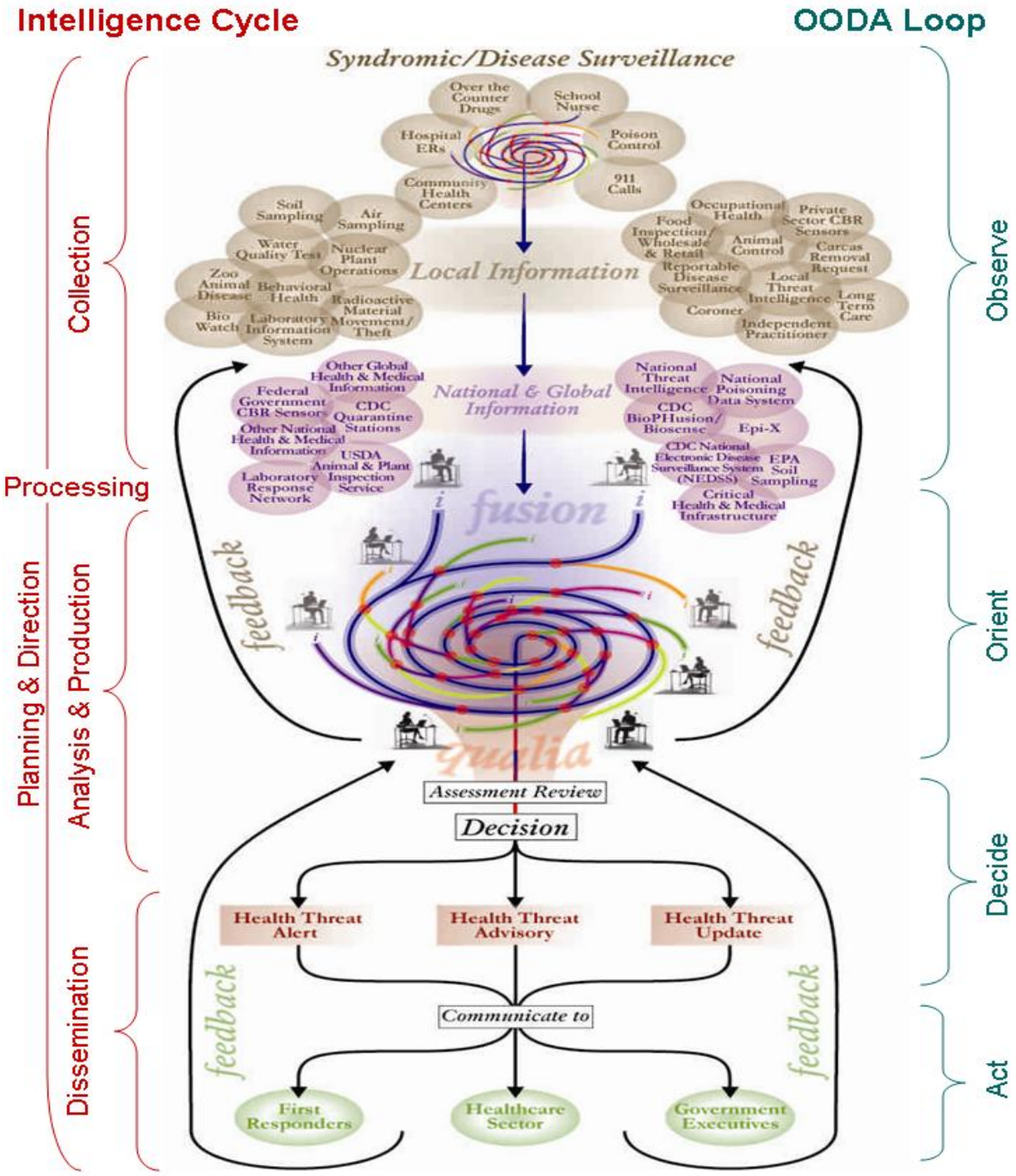


Figure 8. Health Threat Assessment model.

D. MODEL DEVELOPMENT THEMES

During the interview process, despite the variety of individuals interviewed, several reoccurring themes arose that deserve mention. These topic areas were incorporated into the design of the model where possible. Appendix E documents the analysis of these themes by individual interviewed.

1. Layers

One concern was that the data and information input occurs in a number of layers because of the varying nature of the data involved. Some information is automated, while others must be culled. The automated information will likely be received with a steady frequency and standardized data elements. This information is shown as such at the top layer of fusion, called disease surveillance. Because of the routine nature of this data, exceptional data elements are more easily identified than data that is not routinely collected.

In addition, multiple layers of information exist because of the multiple layers of government. The model depicts state and local information separately from that of the federal government. This is appropriate because the scope of information available at the federal level is nationally focused and may assist in developing an understanding of the threats that are external to a particular jurisdiction, but that may affect the jurisdiction in some future period.

2. Thresholds

Several individuals also commented on the establishment of thresholds and the difficulty in doing so. Since this is a relatively new field, the ability to draw on historic data at the state and local levels may be difficult, particularly in areas where data has never been automated. Although all believed that there should be more than one type of emphasis given to finished intelligence, some thought that the ability to distinguish between what would fall into the category of alert over an advisory would most often be subjective. This issue is not incorporated in the model and is a field for future research.

3. Collaboration

All agreed that collaboration was critical to the process. Several raised the issue of connectivity to perform the collaboration, the policies that need to be developed in order to share the information, and the degrees of willingness to share information across cultures. Information sharing with law enforcement is easy to do, but law enforcement sharing information with public health was not viewed as readily apparent. The requirement for development of social networks and trust must be satisfied not only at the analyst level, but also at the health commissioner/police chief/fire chief level or policies will not be implemented to foster collaboration. The concept of collaboration has already been discussed extensively relative to how it has been included in the fusion/qualia portion of the model.

4. Decision Making

Because of the number of individuals ideally involved in the collaboration process, some concern about the identity of the final decision maker arose in multiple interviews. Within the health and medical community, there must be a number of experts involved in the collaboration process because of the highly technical aspects of many categories of information. The question then arises, should the decision maker be an analyst, one of the subject matter experts, or a person outside the process who can consider the intelligence developed from a more objective viewpoint. Based on information obtained through interviews, the decision maker is included in the model as a separate and discrete element following the fusion process. This takes into consideration the need for separation between fusion, which recommends actions, and decision making, which directs actions.

5. Products

Almost all individuals interviewed discussed the issue of products. The format, frequency, and customers were the top concerns raised. In considering format, the options range from hard copy text documents, to text email, to graphic presentations, to web

pages, and while all are options to consider, the decision is based on customer preference. The need for separate products for different groups of stakeholders is presented in the model; however, the format and content of the product is a field for future research.

6. Technology

The availability of technology to conduct the collaboration and the presentation of products represented two additional concerns. Although somewhat related, the analytic process portion of the technology was seen by several as the more difficult of the two. This issue was cited as a task almost too difficult to overcome in rural areas where funding is extremely limited and current levels of automation for data gathering are almost non-existent. The technology available for collaboration and analysis is a topic for future research and is not represented in the model itself.

7. "Real-time" Issue

The last issue to be mentioned is the timeliness of the information. Most disease surveillance only pulls data and analyzes it on 24-hour cycles at the most frequent basis, so emergency care providers may be the only individuals able to notice immediately that an incident is occurring. By definition, aggregation of data infers that some time has passed. Indeed, if the fusion process is done well, it will involve more than one analyst or subject matter expert, which decreases the ability to provide "real-time" value from the information.

E. SUMMARY

This chapter presented a model for the development of a health threat assessment at the state and local level, which was formulated by gathering information through surveys and interviews. The model was then compared to the intelligence cycle and the OODA Loop. The health threat assessment process could occur in fusion centers or through collaborative information sharing technologies with individuals at disparate locations.

V. STRATEGY FOR DEVELOPING AN INFORMATION SHARING CULTURE

> Any change, even a change for the better, is always accompanied by drawbacks and discomforts.
>
> — Enoch Arnold Bennett

A. INTRODUCTION

The concept of developing health threat qualia is new to the intelligence world. The terminology itself is nascent in the published literature.[6] The previous chapters have focused on the model for developing a health threat assessment. This chapter will focus on the strategy for implementation of the model.

B. BLUE OCEAN STRATEGY

Whether developing strategy for military, business, or government, "strategy will always involve both opportunity and risk" (Kim and Mauborgne, 2005, p. 19). The opportunity presented by this strategy is the development of a culture that is rich in information sharing and may ultimately result in health threat qualia. In the intelligence world, however, risk also relates to the necessary balance between information sharing and the compromise of sensitive information.

The first requirement is the need to balance the risk of restricting information distribution due to concerns about the compromise of sensitive information by law enforcement and the consequent inability of the rest of the first responder community to take prevention or preparedness actions because of an absence of information concerning a specific threat. The failure to develop new ways to share information in an effort to understand the nuances of specialty areas, including the health threat, could result in unnecessary disease and injury. In view of the level of sophistication of our current

[6] Other than this paper, Rolka's prepublication work is the only other discussion found regarding this area of intelligence and his work focuses on the development of this concept at the federal level.

ability to develop a robust base of knowledge, however, such an outcome is unacceptable. Since 2001, the intelligence community has been developing technologies that are increasingly collaborative. Still, products and processes devoted specifically to the development of health threat assessments should become the next focus for inclusion in this process.

This next discussion will include the development of an implementation strategy for building a health threat assessment by developing untapped market space, termed the *Blue Ocean Strategy* by Kim and Mauborgne (2005). The focus of their argument is that a blue ocean differs from a red ocean in that red oceans represent current market space or organizational processes. Conversely, blue oceans represent the markets or organizational processes that not currently existent in industry (p. 5). The cornerstone of a blue ocean strategy is the implementation of a new market space based on value innovation, which focuses on the creation of high value through innovation or differentiation, while reducing cost (p. 13). The development of a blue ocean strategy canvas includes consideration of four factors. These factors answer the questions, "What should be eliminated, reduced, raised, and created?" The first two factors eliminate "cost" to the organization while the second two improve "value" (pp. 29-30). The next part of this discussion will focus on addressing these questions as they relate to the development of a health threat assessment.

1. What Should be Eliminated?

Information silos in the intelligence community must be eliminated both between law enforcement and non-traditional intelligence community members as well as between those agencies internal to non-traditional intelligence communities, such as among various specialties in public health.

Currently, information sharing is often restricted based on security and handling classifications, such as "law enforcement sensitive," thus producing or sustaining information silos. A recent example of this is a joint document by the Federal Bureau of

Investigation and the Department of Homeland Security (2008), titled *Domestic Terrorist CBRN Intent and Capabilities Threat Assessment*. The front page of the document contains the handling instructions:

> LAW ENFORCEMENT SENSITIVE: This information is the property of the Federal Bureau of Investigation (FBI) and may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. (p. 1)

When contacted for permission to distribute the document to state and local agencies, the Federal Bureau of Investigation denied distribution to health departments and local health care facilities.[7] This document clearly has public health implications, but sharing the information with public health officials and hospitals, both of which represent communities that play significant roles in the management and treatment of casualties from weapons of mass destruction, is prohibited. According to 20 CFR Part 23, as stated in 1993 Revision and Commentary, the penalty for distribution of these reports without permission is a fine up to $10,000, in addition to any other penalty imposed by law.[8]

In order for non-traditional intelligence community partners, such as health departments, to protect their communities and respond appropriately in the event of an incident, the intelligence community must eliminate this type of restriction in information sharing. According to Natarajan, proposed legislation is pending that would require release of information in an unclassified manner before release of the classified version (Nitin Natarajan, Program Manager, Critical Infrastructure Program, Department of Health and Human Services, personal communication, October 1, 2008, Seattle, WA, at the Director's of Public Health Preparedness Conference); however, the document

[7] This permission was denied by Federal Bureau of Investigation General Council per Unit Chief FBI Domestic Terrorism Analysis Unit per email dated November 15, 2008 with Washington Regional Threat and Analysis Center public health analyst.

[8] 28 CFR Part 23, The statutory authorities for 20 CFR Part 23, as stated in 1993 Revision and Commentary, are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). The Act provides for confidentiality of information as follows: … "(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law."

described is not technically classified, it does contain limiting distribution instructions. As a result, the intelligence community will still be able to restrict distribution by including special instructions on documents labeled “law enforcement sensitive” or other such handling instructions.

As mentioned previously, the health and medical communities also maintain internal information silos. These can include human disease surveillance data within the community of epidemiologists, hospital bed status within the community of hospital administrators, animal disease surveillance data with animal control or veterinary science specialists, and threat information with intelligence analysts. Nevertheless, intra-disciplinary information hording must be eliminated. Truly, to develop qualia regarding the health threat, information sharing and collaboration must be improved.

The creation of information silos results in a cost to the public health and medical community through an inability to develop a true understanding of the health threat. This failure creates second and third order consequences relative to insufficient or inadequate planning and equipping of the community to meet these threats, and such inadequate preparation could certainly cost lives.

There are likely to be as many solutions to the problem of maintaining information silos as there are state and local jurisdictions. However, the crux of the problem is the need to build a collaborative capacity within each organization. Thomas, presents success factors that they observed in a study on inter-organizational collaboration, which can be applied to the intra-organizational setting as well. At least 25% of the participants agreed a “felt need” to collaborate, and a common goal or recognition of interdependence contributed greatly to success. Other factors considered important by participants were social capital, such as interpersonal networks, and effective communication and information exchange. Lastly, participants felt that incentives, such as collaboration as a prerequisite for funding, coupled with strong leadership support were also important (Thomas, Hocevar and Jansen, 2008, p. 6). Although 25% of the participants did not mention trust and competency, other literature indicates the importance of these two factors in reducing intergroup rivalry and

developing strong information sharing practices (Kleinbaum and Tushman, 2008, p. 6). The organizational design components for ensuring information sharing success include the following.

- a common purpose
- a formalized structure to ensure information sharing, such as routinely scheduled meetings and committees
- the ability to share information laterally through technology and interpersonal means
- incentives
- personal attributes, such as competency, commitment, and social trust (Thomas et al., 2008, p. 6)

2. What Should be Reduced?

Because of the lack of information sharing internal and external to the public health community, duplication of effort often exists. In order for a public health intelligence analyst to develop an accurate health threat assessment, access to information regarding the number of data inputs annotated in the model is essential. Without routine access to this information, each possible unusual occurrence will require research into the data, actions that both duplicate efforts and expend valuable time that could be used to develop an appropriate prevention or response.

Duplication of effort or redundancy often results from low trust situations. Covey describes the attributes of low trust organizations, which include situations where people do not share information freely; instead, they hoard information, new ideas are openly resisted, “meetings after the meeting” occur frequently, people feel unproductive tension and sometimes fear (Covey and Merrill, 2006, p. 237). Because of the lack of information sharing due to low trust situations within an organization, individuals will seek out information they need from alternate sources, which results in an unnecessary expenditure of resources. The cost of this duplication of effort creates an unnecessary tax on the organization (Covey and Merrill, 2006, p. 250).

In the public health and medical field, the diverse nature of myriad of specialties involved also can create communication barriers. Highly specialized individuals, by their

nature, are likely to be dysfunctional because of their diversity and their differences in terminology and perspective (Polzner, 2008, p. 20). These communication barriers are likely to result in low trust situations due their divergent goals, territoriality, and competition for resources (Thomas et al., 2008, p. 6).

Because of duplication of effort and lack of information sharing, research may result in incomplete information gathering giving the analyst an inaccurate picture of the situation. As mentioned under information silos, this incomplete or inaccurate understanding may cost lives through a lack of adequate preparedness.

The solution for developing high trust organizations capable of minimizing duplication of effort relies on implementation of processes that overcome the barriers that obstruct information sharing. Kleinbaum and Tushman (2008) suggest investment in idea brokers within the organization. Creating situations in which these individuals can interact may foster the development of relationships across the organization. Such actions help develop the informal networks within the organization as a means of influencing social interaction on a positive scale rather than allowing it to operate at the negative end of the spectrum (pp. 26-27). Numerous authors suggest the development of incentives and rewards for horizontal and vertical information sharing (Thomas et al., 2008, p. 2; Howes and Quinn, 1978, p. 73; Fisher et al., 2008, p. 47).

3. What Should be Raised above Industry Standard?

This research is replete with documentation of the need for collaboration. Collaboration through interagency partnerships is particularly valuable because of the different perspectives that can be brought to bear during analysis when varieties of disciplines are involved in the process. By tapping into social, trust-based networks, the knowledge community gains access to both tacit and explicit knowledge (Von Kortzfleisch, Margel, and Proll, 2007, p. 3). Brafman and Beckstrom (2006) make the analogy that the best organizational design for optimizing this type of information flow is that of a starfish as opposed to that of a spider. The starfish organization represents a network of nodes that will continue to thrive if a leg (network node) is cutoff. However, as with a spider, representative of a hierarchical organizational structure, if the head is cut

off, the organization dies (pp. 34-35). One aspect of starfish organizations is that they usually have informal leaders known as catalysts (pp. 34-35). The power of these individuals is that by having connections across multiple network nodes, they have the effect of bringing them together (Gladwell, 2000, p. 51).

In this aspect, the power of social networks can be substantial. However, knowledge is power and sharing information means sharing of power. Because of this, knowledge management is highly political. In order to be successful, it requires an astute manager to cultivate both the political aspects as well as the informal, trust-based, social aspects of information sharing (Davenport, 1997, p. 188). The greater the social trust in the organization, the less likely politics will have a significant impact on information flow (Covey and Merrill, 2006, p. 251).

Increased collaboration results in an increase in situational awareness. Hansen and Nohria (2006) discuss the value creation that results from collaboration. Among the five major categories are the following.

- Better decision making as a result of advice and information obtained from colleagues
- Innovation through cross-pollination of ideas and recombination of scarce resources
- Enhanced capacity for collective action by dispersed units (p. 5)

Increased situational awareness and collaboration provide analysts with increased information sets, which may result in a more comprehensive threat assessment. The greater the detail in the threat assessment, the better the decision maker will be able to develop appropriate protective measures for his workforce or the population in general. The value created through collaboration lies not only within the public health and medical community, but also between public health and other interagency disciplines as they gain a greater understanding of the implications of various health threats and the necessary precautionary measures leadership can take to protect the workforce. Although initial efforts in collaboration require some degree of trust, the value proposition is that, as we have already discussed, with continued collaboration, the ability to protect the

workforce increases. Increased collaboration and information sharing "are self-strengthening and reinforcing" (Boselego, 2005). This then becomes a cyclic value in the process.

4. What Should be Created that Has Never Been Offered Before?

An environment of operational synergy results from trust and information sharing. Schoenberg (2001) presents the concept that operational synergy is comprised of resource sharing and knowledge transfer in business acquisitions. These two components contribute to value creation because of the synergistic results of these two components (p. 101). The American Heritage Dictionary defines synergy as "the interaction of two or more agents or forces so that their combined effect is greater than the sum of their individual effects, and, cooperative interaction among groups, … that creates an enhanced combined effect" (*The American Heritage® Dictionary of the English Language, Fourth Edition*, 2004). Applying this same concept to the realm of intelligence, operational synergy results when two or more agencies transfer knowledge and share information resources through some type of information sharing process and/or technology.

As the cycle continues, analysts become better-informed resulting in improved health threat qualia. This operational synergy and qualia surrounding the health threat are value innovations that are not currently part of the intelligence community.

A summary of this four-factor framework, as it relates to the development of a health threat assessment, is displayed in Figure 9 (Kim and Mauborgne, 2005, p. 29).

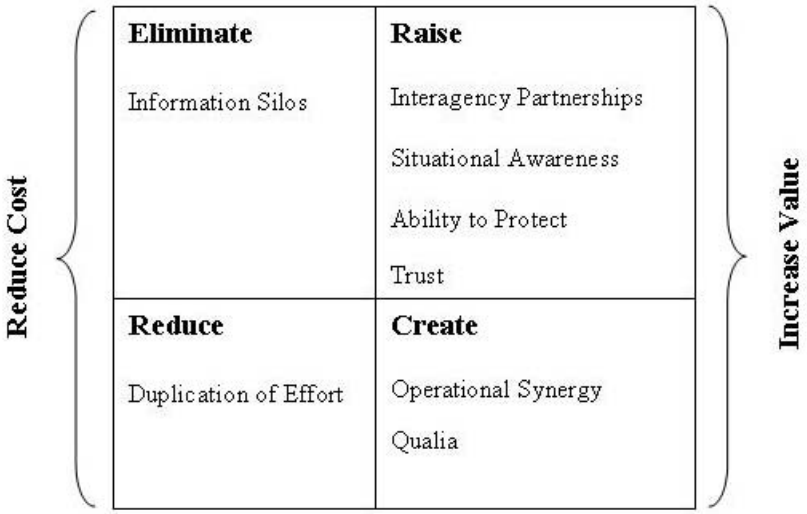


Figure 9. Four-Factor Framework for a Health Threat Assessment Strategy. (From: Kim and Mauborgne, 2005, p. 29)

The layout of this strategy comparing current practice to the value innovation of the development of a health threat assessment is depicted in the strategy canvas in Figure 10. Note the expected improvement in the ability to develop an effective health threat assessment with increase information sharing and collaboration.

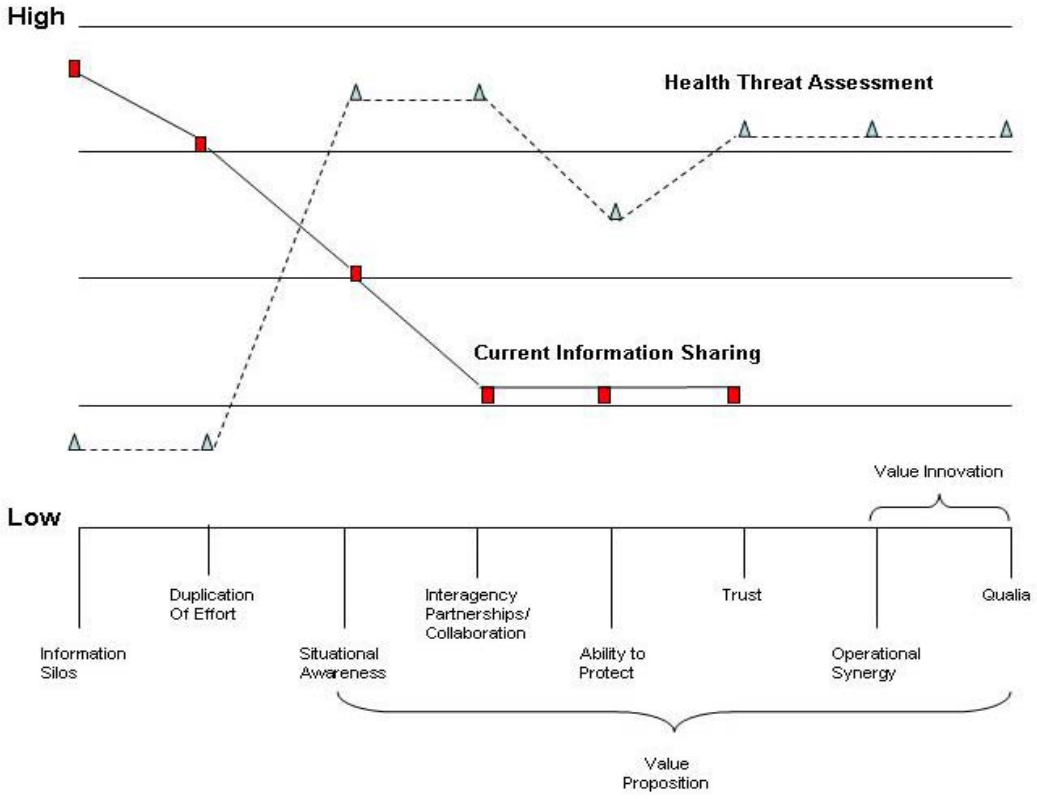


Figure 10. Health Threat Assessment Strategy Canvas. (From: Kim and Mauborgne, 2005, p. 29)

C. OPPORTUNITIES

This strategy emphasizes the value derived from development of information sharing knowledge management systems based on trust and collaboration. The process to reach this goal requires a combination of information technology, changed behaviors regarding information documentation (Smith and McKeen, 2004, p. 25), and changes in information sharing culture (Fisher et al., 2008, p. 27).

1. Federal Emphasis

In recent months, the federal government has placed emphasis on the development of several efforts to integrate health data streams. These initiatives, although

not currently producing information for consumers at the state and local levels, signal that the timing is right for development of similar initiatives at the state and local levels.

The Centers for Disease Control and Prevention is developing several initiatives including BioPhusion. The name of the program plays off the concept of integrating public health with the traditional intelligence concept of fusion. This program intends to integrate the meta-analysis, often thought of as disease or syndromic surveillance, with real-time incident data (Rolka et al., In Press, p. 5).

The Department of Homeland Security has also begun development of an initiative called the National Biosurveillance Integration Center. According to Myers, the Center's Director, the Center's mission is to "integrate and fuse [information] across the domains of health…human, animal, plant and environmental, and apply that to a national security perspective via the nation's critical infrastructure" (Eric Myers, personal communication, October 15, 2008, Denver, CO, at the Health Security Intelligence (HIS) Workshop). The Department also held the Health Security Intelligence (HIS) Workshop in Denver, Colorado from October 14 through 16, 2008. This workshop was held to determine the state of public health information fusion occurring at the state and local levels, and the desired products that the Department of Homeland Security could produce for state and local agencies.

The Defense Intelligence Agency has also altered its operations in a new initiative. The Armed Forces Medical Intelligence Center has recently been renamed as the National Center for Medical Intelligence. Although its primary focus is still overseas, the analysis now includes overseas health threat implications to the United States (Defense Intelligence Agency (DIA), 2008, p. 1). With the expansion of its mission, the National Medical Intelligence Center has also changed its policy regarding access to its unclassified information and has now moved to Intelink-U, thus making make it easier for customers to access their Web site. Users from .mil and some .gov domains do not need to apply for an account (Department of the Army, Fort Detrick, 2008).

2. Economic Downturn

While a period of economic crisis may not appear to be the ideal time to launch a new initiative, the public health implications of the crisis make this a critical time to do so. On November 15, 2008, the headlines of the Washington Post were, "Experts See Security Risks in Downturn. Global Financial Crisis May Fuel Instability and Weaken U.S. Defenses" (Warrick and Tate, 2008, pp. A1, A9). The implications in the story are that terrorism experts see al-Qaeda viewing the economic conditions in the United States as a sign of weakness, thus making it an ideal time for attack. However, another implication that is not quite as explicit is captured in the text below the adjacent photo of a group of Pakistani women "Pakistanis receive handouts of food at a shrine in Islamabad this week. Soaring food prices have sparked unrest" (Masood, 2008, p. A9). The public health implication not stated here is that extreme poverty contributes to increased disease rates in populations and decreased reporting, which means we may not be able to track the next global health threat as it spins its way around the globe. These conditions make the present an ideal time to launch efforts at building support for health threat assessments at the state and local levels. In the District of Columbia, the Washington Regional Threat and Analysis Center (WRTAC) is supportive of the effort to produce separate products geared toward specific audiences, including the health and medical community as well as the fire and emergency medical services communities.

D. CHALLENGES

While current opportunities may make this an ideal time to forge ahead with new initiatives in the intelligence world, such as the development of a health threat assessment model for use at state and local levels, there are still many challenges to implementing the strategy.

1. Trust

In his book, *The Speed of Trust*, Covey and Merrill (2006) open with a discussion of the importance of trust. They refer to several types of trust, including organizational trust, societal trust and market trust (pp. 237-245, 304-305). Trust is the one thing, they

say, that is common to every relationship whether it is personal or business-related. Moreover, if that trust is destroyed, the relationship will disintegrate (p. 1). This could not be truer than in the intelligence community. Information gathering, and therefore information sharing, is the tradecraft of intelligence analysts. However, since analysts are rarely the generators of information, they must rely on others to provide them with that information. Trust is critical in this exchange of information. Cooper (2005) states that investigations into intelligence failures cite information sharing problems as being the crux of the issue. The recommendations for improving information sharing were to establish new authorities mandating information sharing and new information technology. However, he advises that "effective collaboration is fundamentally a matter of culture and values; what is needed is…to forge expert social networks and effective 'distributed trust' systems" (pp. 55-56).

As may be seen from the previous discussion of the FBI's restriction on the release of threat assessments with obvious implications to the public health community, there is still a significant need for improvement in the degree of trust between federal government law enforcement agencies and non-law enforcement, state-level agencies.

2. Collaboration

a. Technology

One of the more difficult problems with implementation of new information technology concepts is the "hype cycle." The Gartner Group documents four phases of acceptance after the initial launch of "the good idea trigger." The first phase ends with the peak of inflated expectations. A drop quickly follows to almost pre-launch acceptance levels, referred to as the trough of disillusionment, which results from the realization that the project will not be the solution for all problems. Management may respond with renewed emphasis on the value of the project or adjust the original project plan, which results in a gradual increase in acceptance, termed the slope of enlightenment. With continued emphasis and adjustment, the project concept will continue to rise until a plateau of productivity is reached. Smith and McKeen (2004)

state, **"**Long-term sustainable value can only occur by reassessing and reevaluating what needs to be done to address the problems and complexities involved and to refocus on ways that will simplify and add value" (p. 27). Figure 11 depicts the hype cycle.

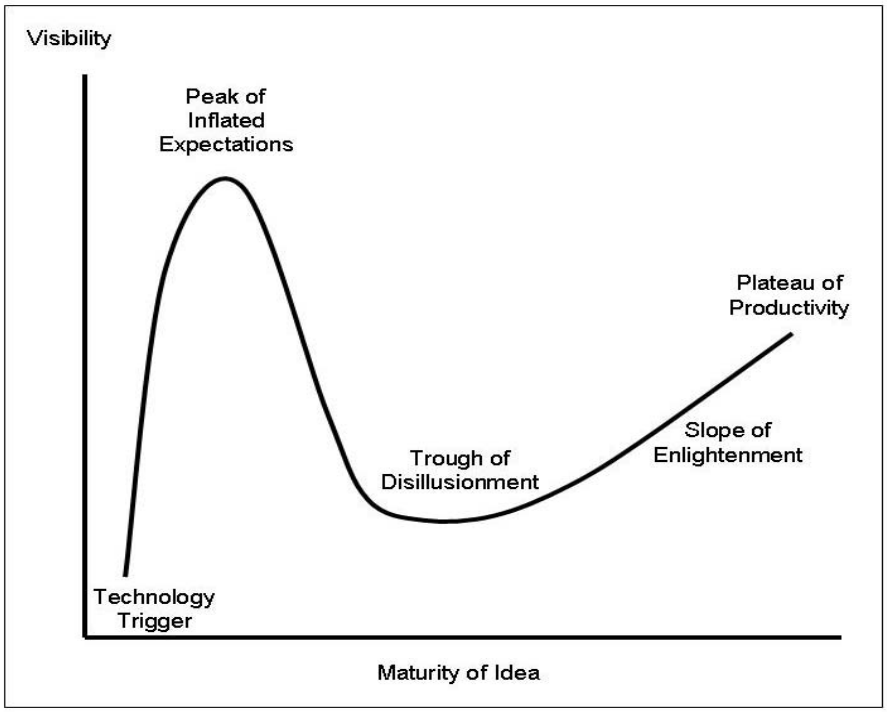


Figure 11. Gartner Hype Cycle. (From: Smith & McKeen, 2004)

b. Social Network

In *The Hidden Power of Social Networks*, by Cross and Parker (2003), the authors discuss that the value of a network lies in understanding two aspects of it; first, *who knows what* and second, *how to get access to them* (pp. 36-37). In the evolving technological world of the intelligence cycle, it does not matter how much any individual knows, if no one else knows that they know it. This is why the social network is so important. The information sharing of the social network relies on the relationships that have been built and the attitude toward knowledge sharing (Chow and Chan, 2008, p. 462). According to Wasko and Faraj (2005), in the information technology arena,

> Organizational members benefit from external network connections because they gain access to new information, expertise, and ideas not available locally, and can interact informally, free from the constraints of hierarchy and local rules. Even though the employing organizations may be direct competitors, informal and reciprocal knowledge exchanges between individuals are valued and sustained over time because the sharing of knowledge is an important aspect of being a member of a technological community. (p. 36)

In the intelligence world, social networks are somewhat different from ordinary business or industry, because knowledge is their sole stock in trade and that knowledge is vital to ongoing investigations and other homeland security issues. Therefore, relationships in the intelligence world are based on a degree of trust, which must exceed that of most business relationships. Therefore, the problem becomes the ability of connectors to link other individuals together in such a way as to pass on that trust. One recommendation by Cooper (2005) is the use of journeymen who have had years of experience in the intelligence field to act as mentors and guides for junior analysts and those outside the traditional intelligence community (pp. 51, 56). Another recommendation is a complete restructuring of the security clearance structure making security clearances universal in order to facilitate information sharing across the intelligence community (p. 57).

3. Privacy

The collection of information about an individual's health status by governmental agencies who then further share that information with other agencies may raise concerns among consumer advocacy groups. Although significant steps have been taken on the part of public health officials to de-identify data, there is a possibility that when health data is combined with law enforcement or other governmental databases, the ability to identify the individual may be possible. An example of a public health information system in which privacy concerns are substantially addressed is the ESSENCE II system.

ESSENCE II is a syndromic surveillance system that allows for daily analysis of outpatient data from District of Columbia area military and civilian treatment facilities (Lewis et al., 2002, p. 181). Because of the need to maintain individual privacy, Johns

Hopkins Applied Physics Laboratory, the developers of the system, considered the process of "anonymization" in the development of the ESSENCE II system. Lombardo (2003) provides an excellent discussion of "anonymization" or de-identification of the various data categories due to their sensitivity. There are three data categories, namely traditional surveillance data, nontraditional clinical, and nontraditional nonclinical. The only category that requires anonymization is the nontraditional clinical data (p. 329).

Samarati and Sweeney (Unpublished) developed a process known as k-anonymity to protect patient privacy. This process acknowledges that even though data may have had names and social security numbers removed, someone could still trace patient identification through comparison with other publicly available sources. K-anonymity is "the degree of protection of data with respect to inference by linking data." In their process, data is de-identified through suppression of data fields and generalization of data. Because of this detailed de-identification of data, the data collection and use complies with the Health Insurance Portability and Accountability Act (HIPAA).

In addition, all surveillance systems within public health are now required to be Public Health Information Network (PHIN) compliant. The Public Health Information Network (PHIN) is a major initiative from the Centers for Disease Control (2008) to provide standards-based disease reporting and public health information management. PHIN 2.0 requires that each state "ensure that its electronic information systems … are secure and available at all times and the information contained is only accessed or used by authorized users for authorized purposes." This access restriction as well as restriction from patient identity ensures individual privacy while still providing an extensive system of disease surveillance.

Although no system is 100% secure, ESSENCE II has attempted by design to prevent SQL Injection from being possible. Data collection is done using Secure FTP (SFTP) or HL7 over secure virtual private network (VPN) tunnels. However, if intrusion does occur, ESSENCE II logs user activity that can be used for follow-up investigations of potential break-ins (Rekha S. Holtry, Johns Hopkins Applied Physics Lab, personal communication, 2008).

All future systems designed for information sharing of individual patient information must also meet this level of effort of privacy protection to reassure the public that analysts will not compromise their health information in the intelligence development process.

4. Urban vs. Rural Availability of Resources

Another challenge to the development of a health threat assessment at the state and local level is that of the differences in availability of data in rural verses urban areas. Rural areas often do not have automated outpatient patient data from hospitals or real-time reporting systems. The method of reporting may be in manual format, originating with the individual health-care provider or local hospital, passing through the local health department, which then processes the information within a specified period per the states reporting guidelines, before passing it up to the state level (Kraig Humbaugh, Director of the Division of Epidemiology and State Planning for the Commonwealth of Kentucky, personal communication, October 2, 2008, Seattle, WA at the Director's of Public Health Preparedness Conference). This process, however, can vary widely depending on the state. In the District of Columbia, required reporting times vary from two to 48 hours depending on the disease while in Kentucky, the timelines vary from 24 hours to five days (District of Columbia, Reportable Diseases in the District of Columbia, 2008; Kentucky, Reportable Disease in Kentucky, 2008).

E. SUMMARY

This chapter presented an implementation strategy for the development of a health threat assessment. The strategy includes a four-factor framework for reduction of costs and increase in value. The factors that reduce costs include the elimination of information silos and the reduction of duplication of effort. The factors that increase value to the organization through the value proposition include increasing interagency partnerships, situational awareness, trust, and the ability to protect. In addition, the value innovations to the organization are the creation of operational synergy and qualia.

Internal and external opportunities and challenges may affect the strategy's implementation. Opportunities that may favorably affect the implementation are the current federal emphasis on developing biological surveillance systems and the economic crisis that may exacerbate disease conditions around the world. Challenges that present obstacles to implementation are overcoming the cultural issues that inhibit trust and collaboration between the intelligence community and non-traditional partners. Other challenges include the need for protection of data for privacy considerations, and the availability of information in rural areas due to limited automation of data streams. Public health officials must consider these opportunities and challenges prior to implementation of a process for development of a health threat assessment.

VI. RECOMMENDATIONS

> The IC [Intelligence Community] must transform itself into a community that dynamically reinvents itself by continuously learning and adapting as the national security environment changes. It has elucidated the principles from an exceptionally rich and exceedingly deep theory (Complexity Theory) about how the world works and has shown how these principles apply to the Intelligence Community. These principles include self-organization, information sharing, feedback, tradecraft, and leadership. (Andrus, 2008, p. 6)

A. INTRODUCTION

This thesis contributes to homeland security through the development of a model for a health threat assessment. This model demonstrates the need for the public health and medical community to breach barriers that will improve collaboration across sectors to produce a more secure homeland. This can only be accomplished through trust, which must be developed through strategic leadership, complete transparency, and clarification of expectations in order to establish the consummate information sharing community and, thereby, qualia.

B. RECOMMENDATIONS

Individuals from the private sector and local, state, and federal government have validated the model for the development of a health threat assessment; however, further work is necessary. Based on the interviews and analysis conducted, I recommend policy development and future research in the following areas.

1. Barriers to Information Sharing

The intelligence community must eliminate barriers to information sharing between itself and non-traditional partners such as public health through relaxation of current distribution policies for “For Official Use Only” and “Law Enforcement Sensitive” products. The example of the Federal Bureau of Investigation denying

dissemination to public health departments information related directly to domestic terrorists' capabilities to use chemical, biological and radiological weapons demonstrates the gap that the intelligence community must still close.

2. Public Health Information Sharing Policies

State and local fusion centers and health departments must develop information sharing policies that address health information concerns specifically. Carter (2005) emphasizes that "agencies must establish policies with respect to what types of data they will impart and to whom" (p. 3). Many of the interview participants at the state and local levels acknowledged that they did not have formal written policies for information sharing either internal or external to their agencies. While this appeared usually to allow for greater information sharing than at the federal level, decision makers appeared to base their policies on personal preference rather than routine or documented practices. Without formal written policies, consumer advocacy groups could view information sharing with other non-medical entities as infringement on personal privacy concerns. If not reviewed against documented criteria, agencies could inadvertently release information to entities that could use it against government officials. Therefore, state and local public health agencies should establish formal information sharing policies.

3. Health Threat Assessment Products

The Department of Homeland Security or Department of Health and Human Services should sponsor future research regarding the type, format, frequency, and content of intelligence products at the state and local levels for the variety of entities requiring health threat assessments. Considerations regarding the type, format, frequency, and content of intelligence products have been the subject of significant debate within fusion centers. NYPD SHIELD is an example of a product that is generally accepted as a good format. Most importantly, the aspect of NYPD SHIELD that makes it such a successful product is that it provides implications for New York City.

However, most interview participants agreed that a single product would not meet the needs of the variety of audiences that should receive health threat information. The

implications for the jurisdiction are critical in each product, but those implications vary depending on the audience. The individual first responder has a need for immediate tactical information regarding the threat to their own personal safety; therefore, the frequency and method of delivery of threat information is likely to be more important to them than other entities. The private and non-profit sectors of hospitals and community health centers have a need for operational level information, likely geared toward their ability to diagnose and respond. Lastly, the executive level of government must receive more information related to strategic planning so that it can ensure that systems are in place to detect, investigate, and respond in order to mitigate casualties. Therefore, the solution probably lies in the use of a variety of formats for a health threat assessment.

4. Technology for Facilitation of Information Sharing

Department of Homeland Security or Department of Health and Human Services should sponsor research into types of technology that can best support the new information sharing and collaborative structure necessary for state and local jurisdictions to develop comprehensive health threat assessments. From previous research, it is likely that a suite of information technology solutions will be necessary for application within each state. Due to the recent trend in reduction of federal funding through both the Hospital Preparedness and the Public Health Preparedness Cooperative Agreements established within Department of Health and Human Services, upon completion of research and pilot studies, state level agencies must be adequately funded to support this initiative.

5. Thresholds

Department of Homeland Security or Department of Health and Human Services should sponsor research into a methodology for establishment of thresholds that queue homeland security professionals that an exception to an established pattern or a sentinel event has occurred. Since this is a relatively new field, the ability to draw on historic data at the state and local levels may be difficult, particularly in areas where data has never

been automated. Therefore, the study of algorithms or other mathematical models that could locate exceptions within a variety of information sources would be advantageous to those nascent in the intelligence development process.

C. CONCLUSION

The timing is right for state and local public health and medical agencies to begin to develop health threat assessments for their jurisdictions. Emphasis within the federal government portends the need for data gathering at the state and local levels. Because state and local governments are more apt to be able to understand the complex implications of the "street level" information that is available to them, they are in a better position than most federal agencies to aggregate, share, and fuse such information. In addition, due to the likelihood that information owners at the tactical level have familiarity and interdependent relationships with each other, they also share trust and a willingness to collaborate. Therefore, the development of health threat qualia is more likely to occur at this level.

It is clear from the arguments presented in this thesis that health and medical intelligence belongs in the mainstream of the intelligence community in order for us to maintain a decision advantage, particularly at the state and local level where the intelligence developed will provide the most benefit to first responders and the local community.

APPENDIX A. HEALTH AND MEDICAL INFORMATION SOURCES (NATARAJAN, 2007)

Data Set	Currently Collected	Priority	Detection/Response
Animal Control	Yes	Tertiary	Detection
Radiation	Yes	Primary	Detection
Nuclear	Yes	Primary	Detection
Disease Surveillance	Yes	Primary	Detection
Syndromic Surveillance	Yes	Primary	Detection
School Health Surveillance	Yes	Secondary	Detection
BioWatch	Yes	Primary	Detection
Federal Government Sensors	Yes	Primary	Detection/ Response
Department of Defense Sensors	Yes	Primary	Detection/ Response
Private Sector Sensors	Yes	Tertiary	Detection/ Response
Veterinary/zoological	Yes	Secondary	Detection
Agricultural data	No	Secondary	Detection
CDC Quarantine Station	Yes	Primary	Detection
Pre-hospital Care Diagnosis	Yes	Tertiary	Detection/ Response
Poison Control	Yes	Primary	Detection
Aeromedical Evacuation	No	Secondary	Detection/ Response
Water Testing	Yes	Secondary	Detection
Hospital Bed Status	Yes	Primary	Response
Hospital Critical Asset Survey	Yes	Tertiary	Response
Hospital Capabilities	No	Secondary	Response
BioSense	Yes	Primary	Detection

Data Set	Currently Collected	Priority	Detection/Response
Nursing Home	No	Secondary	Detection
Air Sampling	Yes	Tertiary	Detection/ Response
Occupational Health	Yes	Tertiary	Detection/ Response
Background Illness Levels	Yes	Primary	Detection

APPENDIX B. HEALTH THREAT ASSESSMENT SURVEY[9]

1.

A fundamental responsibility of the government is to detect, prevent, investigate, and respond to criminal and terrorist activity. Incumbent to this responsibility is to also protect residents from naturally occurring threats and disasters. An integrated health threat assessment is an effective tool to ensure this responsibility is achieved. The Department of Health is augmenting the Washington Regional Threat Analysis Center with a public health intelligence analyst to provide medical surveillance and situational awareness to first responders and health care professionals to ensure the safety of DC residents. The purpose of this survey is to aggregate all relevant departments (medical, environmental, veterinary, etc) data sources, information systems and/or reports for a consolidated analysis that forms the basis for an integrated health threat assessment.

Your participation in this survey is voluntary and at any time you may terminate your participation without penalty. All information collected by this survey will be secured and maintained in accordance with District of Columbia standards for confidential or For Official Use Only documents.

1. What data source or information system within your organization contains health or medical surveillance or situational awareness information (i.e. ESSENCE for human disease surveillance)?

2. In what form is this service/product available?

- ☐ Report
- ☐ Map
- ☐ Chart/graph
- ☐ Spreadsheet
- ☐ Database
- ☐ Other (such as write it yourself, please specify)

3. How often is this service/product available?

- ☐ Daily
- ☐ Weekly
- ☐ Bi-weekly
- ☐ Ad Hoc
- ☐ Monthly
- ☐ Other (please specify)

4. What data sources are necessary to produce this service/product such as hospital emergency department data, veterinary visit data, etc?

[9] The original source for these questions was a survey designed in 2007 by Daniel Thomas who worked as a consultant for the Office of the Chief Technology Officer, District of Columbia Government during the developmental phases of the Washington Regional Threat Assessment Center.

*** 5. Who are authoritative sources (POC)for this service/product?**

Name:

Email Address:

Phone Number:

6. Is the final product or service an analysis of the data or is only raw data available?

- [ ] Yes
- [ ] No

7. Are there restrictions on sharing source material with other organizations?

- [ ] Yes
- [ ] No
- [ ] If yes, describe

8. For data analysis does your organization provide labor to produce this product/service?

- [ ] Yes - Skip to #10
- [ ] No

9. Could data be passed to public health intelligence analyst for tabulation and analysis ?

- [ ] Yes
- [ ] No (please explain)

10. What would method of transmission be?

- ◯ Telephone
- ◯ Fax
- ◯ Email

11. Are any formal agreements necessary to access source data or gain labor support to produce this product/service?

- [ ] Yes
- [ ] No

12. What type of digital data certificates, permissions or security clearances are required in order to handle information or product/service?

13. Are any special processes necessary to generate this service/product?

☐ No

☐ Yes

If yes (please specify)

14. Is any specific communication or technology capability necessary to produce this service/product?

☐ Yes

☐ No

If yes (please specify)

15. Are there associated start-up or ongoing costs associated with producing the service/product?

☐ Yes

☐ No

If yes (please describe)

16. If the answer to question number 15 is yes, is product or service federally grant funded?

☐ Yes

☐ No

If yes, what grant?

17. Are there other medical organizations (other than those listed above) that you believe should participate in the development of the Health Threat Assessment?

18. An integrated health threat assessment would result in a change in epidemiological investigative priorities at the state or local level.

- ☐ Strongly Agree
- ☐ Agree
- ☐ No Answer
- ☐ Disagree
- ☐ Strongly Disagree
- ☐ Not Applicable

19. An integrated health threat assessment would result in more informed decisions concerning posture and vigilance for all relevant District Departments (MPD, EMS,DOH, Health Care Facilities, etc)

- ☐ Strongly Agree
- ☐ Agree
- ☐ No Answer
- ☐ Disagree
- ☐ Strongly Disagree
- ☐ Not Applicable

20. In your opinion, what is the benefit of a health threat assessment to your organization?

*** 21. Who is the best Point of Contact for further information concerning this project?**

Name:	
Company:	
Address:	
Address 2:	
City/Town:	
State:	
ZIP/Postal Code:	
Country:	
Email Address:	
Phone Number:	

Your assistance with this survey is greatly appreciated. Please address all questions to:

Beverly Pritchett
Senior Deputy Director
DC DOH
(w) 202-671-6586
(c) 202-380-6586
beverly.pritchett@dc.gov

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. INFORMATION PROCESS FLOW MODEL INTERVIEW - DATA COLLECTION INTERVIEW QUESTIONS

Thank you for taking the time to be interviewed. You have been identified as a subject matter expert, supervisor, or someone who uses or collects health or medically related data in an operational environment. This interview will be used to evaluate a model that I have developed to document the information process flow in the development of medical intelligence through with the final product being a health threat assessment. This type of assessment is intended to assist decision-makers in the determination of protective measures for both first responders and for the general public in order to safeguard against health threats whether they are terrorist related or as a result of natural conditions.

This interview is being conducted pursuant to an approved thesis proposal for the Naval Postgraduate School's Center for Homeland Defense and Security Master's Degree program sponsored by the Department of Homeland Security (DHS). To comply with the Naval Postgraduate School's policies and procedures, this interview must be recorded and a transcript of the interview made.

Any information that is identified as For Official Use Only (FOUO), Controlled Unclassified Information (CUI), or Law Enforcement Sensitive (LEA) Information will be appropriately labeled and protected.

The following questions are being provided to you in advance, so you can adequately prepare for the interview.

1. For the record, please state your name, position, and agency.

2. For background purposes, could you answer the following questions

    a. What is the function of your organization?

    b. What is your role within the organization?

    c. What would you say your area of expertise is?

3. Does your organization collect health or medically related data that could provide situational awareness regarding a health threat to first responders or the general public?

4. What data sources are those?

5. Regarding data sources:

    a. How often do you access them?

    b. How do you use the data?

    c. Is it automated?

    d. If so, how is it automated?

        1) Commercial software?

        2) Organization specific software?

        3) Is there a product that is produced that could be shared with other organizations?

    e. If it is not automated, how is it documented and tracked?

        1) Electronically?

        2) Manually?

6. Does anyone conduct analysis of data for your organization?

7. If so, what are the procedures exist for data collection, analysis and dissemination?

8. If the data is incident related, how is the data disseminated as it relates to pre, during and post incident?

9. Who receives the data?

10. Does your organization conduct surveillance or modeling?

    a. If so, please explain to me the methodology that you use.

11. Looking at the diagram regarding information flow in the development of a health threat assessment:

    a. Are there other data sources not listed that you think should be added to the diagram that would be of benefit to the Health Departments and Fusion Centers to provide health situational awareness?

b. Do you know who collects that data?

c. If so, do you know who they share it with?

d. Do you think that this accurately reflects a possible flow of information? If not, what would you change?

12. What problems and/or concerns do you foresee in the development of a health threat assessment as I have described it to you?

13. What do you think that the benefits of a health threat assessment would be?

14. Is there anything else you would like to add that I may have not mentioned today?

15. What recommendations would you make to DHS to enhance or modify the sharing of health related situational awareness data as it exists today?

Again, thank you for taking the time to prepare for our upcoming interview. Please feel free to contact me if you have any questions. I can be reached via e-mail at beverly.pritchett@dc.gov or via telephone at the following telephone numbers:

202-671-0481 (w)
202-380-6586 (c)
202-671-0857 (conference call)

Beverly Pritchett
Senior Deputy Director
Health Emergency Preparedness and Response Administration
District of Columbia
Department of Health

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. INFORMATION PROCESS FLOW MODEL INTERVIEW - INTERVIEW QUESTIONS

Thank you for taking the time to be interviewed. You have been identified as a subject matter expert, supervisor, or someone who uses or collects health or medically related data in an operational environment. This interview will be used to evaluate a model that I have developed to document the information process flow in the development of medical intelligence through with the final product being a health threat assessment. This type of assessment is intended to assist decision-makers in the determination of protective measures for both first responders and for the general public in order to safeguard against health threats whether they are terrorist related or as a result of natural conditions.

This interview is being conducted pursuant to an approved thesis proposal for the Naval Postgraduate School's Center for Homeland Defense and Security Master's Degree program sponsored by the Department of Homeland Security (DHS). To comply with the Naval Postgraduate School's policies and procedures, this interview must be recorded and a transcript of the interview made.

Any information that is identified as For Official Use Only (FOUO), Controlled Unclassified Information (CUI), or Law Enforcement Sensitive (LEA) Information will be appropriately labeled and protected.

The following questions are being provided to you in advance, so you can adequately prepare for the interview.

1. For the record, please state your name, position, and agency.

2. For background purposes, could you answer the following questions

    a. What is the function of your organization?

    b. What is your role within the organization?

    c. What would you say your area of expertise is?

3. Does your organization collect health or medically related data that could provide situational awareness regarding a health threat to first responders or the general public?

4. What data sources are those?

5. Does anyone conduct analysis of data for your organization?

6. If so, what are the procedures exist for data collection, analysis and dissemination?

7. If the data is incident related, how is the data disseminated as it relates to pre, during and post incident?

8. Who receives the data?

9. Do you interface with other health related organizations?

    a. If so, is your interface on a formal or informal basis?

    b. Is your interface for the purposes of sharing medical or health related information in order to provide situational awareness?

10. What information do you OR would you like your organization to share?

11. Who do you OR would you like to share the information with? (Coordinated with other Federal, Regional, State, and Local response partners)

12. Is any of the data that you collect and/or share classified?

13. What are your policies for information sharing?

14. The diagram that I have provided you depicts an information flow model for fusion of health related information.

    a. What are your initial reactions to the diagram?

    b. The concept of fusion is somewhat amorphous. It has been described as the process of data sources to produce a concept that is greater than the sum of its individual data input. Do you think that this diagram accurately reflects the combining of multiple data sources for sharing with a number of jurisdictional partners to produce fusion?

    c. If not, what would you change in the diagram?

15. One method of sharing data in this manner is to use a wiki. Would you or others in your organization use a wiki or common server/drive to share information with other organizations?

16. Are there any concerns that you or your organization would have for using/posting information to a “wiki” or common server/drive?

17. Are there any other data sources or organizations that you are aware of that would be of benefit to Departments of Health and Fusion Centers to provide situational awareness and development of health threat assessments?

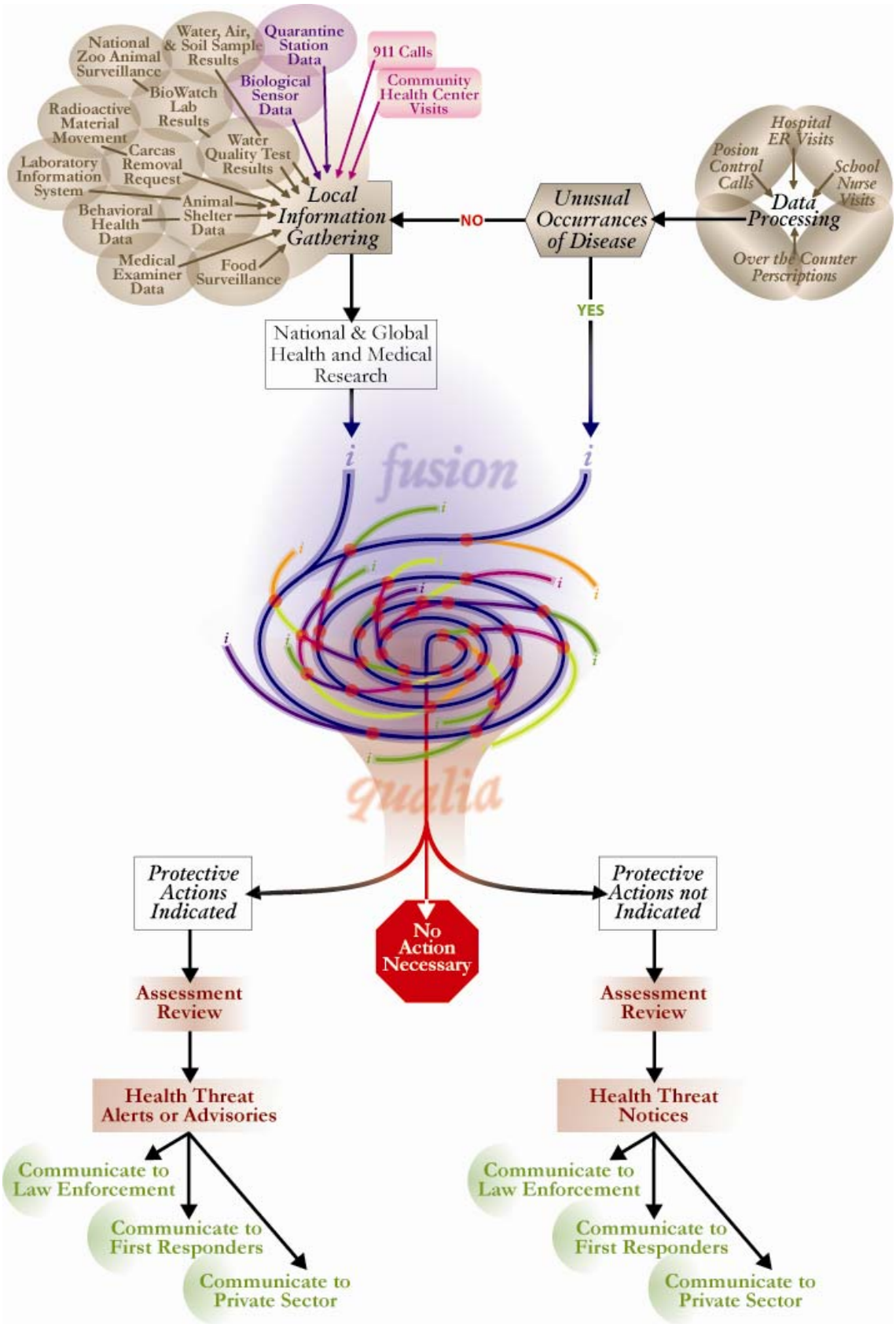
18. Is there anything else you would like to add that I may have overlooked?

19. What recommendations would you make to DHS to enhance or modify the sharing of health related situational awareness data as it exists today?

Again, thank you for taking the time to prepare for our upcoming interview. Please feel free to contact me if you have any questions. I can be reached via e-mail at beverly.pritchett@dc.gov or via telephone at the following telephone numbers:

202-671-0481 (w)
202-380-6586 (c)
202-671-0857 (conference call)

Beverly Pritchett
Senior Deputy Director
Health Emergency Preparedness and Response Administration
District of Columbia
Department of Health


National Zoo Animal Surveillance
Water, Air, & Soil Sample Results
Quarantine Station Data
911 Calls
Biological Sensor Data
Community Health Center Visits
BioWatch Lab Results
Radioactive Material Movement
Water Quality Test Results
Carcas Removal Request
Laboratory Information System
Animal Shelter Data
Behavioral Health Data
Local Information Gathering
Medical Examiner Data
Food Surveillance
NO
Unusual Occurrances of Disease
Hospital ER Visits
Posion Control Calls
School Nurse Visits
Data Processing
Over the Counter Perscriptions
YES
National & Global Health and Medical Research
fusion
Qualia
Protective Actions Indicated
No Action Necessary
Protective Actions not Indicated
Assessment Review
Assessment Review
Health Threat Alerts or Advisories
Health Threat Notices
Communicate to Law Enforcement
Communicate to First Responders
Communicate to Private Sector
Communicate to Law Enforcement
Communicate to First Responders
Communicate to Private Sector

APPENDIX E. INTERVIEW CODING

EXPERT	COMMENT
LAYERS / CLASSIFICATION	
EM	What we have done in the National Biosurveillance Integration Center…is that we have clearances that are at all three levels of classification. So UNCLASSIFIED, SECRET and then TOP SECRET SENSITIVE COMPARTMENT INFORMATION. And that is our attempt is to make sure we are going after those minute tidbits from the intelligence community, from the intelligence from information at all layers that can protect it…A critical piece of PCII, Protected Critical Infrastructure information from the private sector all wraps into that.
EM	I really appreciate the way you have depicted things…because this is trying to get at something that is not traditional laying it out … I think any layer could be a set of layers where you were able to explode this. So, I find this to be very intriguing.
THRESHOLDS	
BB	[If] you selected measles as an agent, you need help…it doesn't meet any of the thresholds to become an effective bio weapon. There is a high immunization status in this country …it is just not going to work.
EM	The process that we are doing … follows very much an analytic process … as data is coming in, it is a 24/7 operations for us so that we have a watch officer on the Department of Homeland Security National Operations Center floor, so that we are in the constant read screen, enter data, or watch data coming into the database and running queries against it. It is a very iterative type process. As opposed to let it run for three days and then we will take a look and see if we have an elephant, a snake or a giraffe. So, number one, introduce the analytic process early and often. And then, by setting up parameters what we do is … find what the facts are in the data, separate those from the assumptions and separate those from the analysis and try to keep those clear among the three. … what we establish … [are] critical information requirements - Classic CIR'S. With the … participants that are in the game already … setting thresholds, which is a stickler, to get those thresholds. But, when you have those thresholds, when you have decided what goes into reporting as opposed to monitoring, as opposed to halt … we try to make those decisions very keenly, based on time, space and resources.
EM	There were two aspects if you will. In my mind, there is a scientific aspect of it that says okay, this threshold is enough so that enough of the population, human, animal, plant, environmental, but enough of the population of things [that] are threatened by the spread of this disease. You take an extreme case like an H5N1, pathogen, and the statistics shown on the wall about people not showing up for work, and comparing it to the 1918 influenza, etc. The other aspect is operational.

	So, we took scientific standards and from the "Bigs" if you will, Centers for Disease Control and the Food and Drug Administration, and AFIS and FSIS, and all of those component elements and said okay you have got to really help us set up first thresholds. By the way, these will be recalibrated as we go … Operationally, the DHS National Op[erations] Center, the NOC, brought together at least … 55 Op[erations] Centers in the greater Washington Capital Region and what they did was … established … [a] steady state, Phase I, II and III. They categorized phases … you go from a steady state, to a Phase I, II, III of increasing severity concern and danger and back to reconstitution, to a Phase I, and we tied our scientific thresholds to those phases … And what that helps with, rather than just being a scientific … but when you look at it from an Op[erations] perspective, and you say … if that occurs, the Secretary of Homeland Security is going to [have to] make some decisions. People are going to be moving. We are going to stop doing certain things. We are going to do other things based on your agency and your mission … Or, let's say there is a significant terrorist attack, you know we are into Phase III. We went from steady state to Phase III…not only then how do you look at those two factors, but how do you look at it when you jump from a phase and completely over one that would let you gradually look at it to a cataclysmic type of thing. And also not forgetting the recovery at the end. Now hopefully, that is simple enough … to make it workable. I am afraid if you make the formula become much more complex … you don't get anywhere. It becomes a theory and it becomes a study as opposed to practice.
KH	In Louisville, they have specific product, in other words, they have thresholds. And you can see a graph of [it], and they already know based on past data that the weekend of the Derby they are going to see just that many more ambulance runs … they already know there is going to be a spike but the question is, is the spike much greater than in past years on Derby weekend.
KH	If you are just looking at syndromic surveillance alone, that is not going to give you the whole picture, so…thresholds are artificially created.
KH	The issue is about thresholds because the thresholds are arbitrary. But, somebody has got to set the threshold. Then if it goes over a certain threshold … you have to look at … other data sources … and you have to look and say, are we seeing increases in any of these other types of data sources? If they start popping up, then I think you have to use common sense and say yeah, we have to go investigate this further.
JD	I'd love to see trend information about where is the flu in relation to our population, historically, and if it's doing this tomorrow, it's going to mean these many more people are reporting to emergency rooms. Yes, and even 24 hours notice, I think, gives us an opportunity to maybe take an action, and I'm not sure what the action is, but we've never had that good information on things like that to allow us to try to adapt.
COLLABORATION	
JG	I was just talking to somebody today who was at the PHIN Conference who recognized one of my employees from the State of Florida who did a superb job in sharing the products that they have developed. And also, in the New Jersey

	Conference two years ago, the Council of State and Territorial and Epidemiologist, one of my staff members shared a system that they used for disease recording mechanisms for the British Virgin Islands, which they were thrilled to tag on to our system and become a user in that.
KH	On the on the other hand we have not seen that there is a replacement necessarily for astute clinicians for us to spend all of the time and resources and we have those limited resources. There is also the issue of the partners and the collaboration that you need … we have had a struggle convincing homeland security that health data is an important part of what they call their fusion center … but I think they [think] of … intelligence from a law enforcement perspective only … I think it could be valuable if they included … health data in their Fusion Center but it is often difficult to overcome that barrier.
EM	Along with this entrée into the law enforcement, public health and intelligence triangles are starting to show up at the fusion centers.
EM	The integration [that] the NBIS is looking for is to be a … set of vector arrows or curves or swirls and I don't think it is vector arrows. And I do believe it is curves and swirls, it is that analytic process.
DECISION-MAKING	
CD	Part of the beauty of what we are developing in the District is a multi-faceted approach to getting diverse information, all which has its own impact and importance to the community's response to a disaster. The ED Connectivity Family Reunification project's value is on taking a set of data, fundamentally a patient's name and a set location and sending it to those persons who are going to be fielding the questions from the public looking for a loved one. The HIS system, on the whole goes much further than simply collecting patient information. And would allow a more insightful look into the state of beds in the District of Columbia, the state of available resources in the District of Columbia. Whether it is people or various types of things, equipment, supplies, medications and the like. So, really it is the combination of the two programs that would allow the Emergency Managers to have a teleconference to discuss the situation or certainly would provide some needed information for critical decision making by the senior policy group.
DG	I think you would have to make a decision whether or not you want to go with a model in which there is a central fusion cell or whether fusion would take place in general in a disbursed way and then what the requirements are to have a core fusion center. But, at some point beyond this large scale fusion of all of these, there would be in fact fusion models taking place at those levels.
DG	I think at some point there is the overriding of the pure WIKI process by having someone say wait a second this is right or wrong … as opposed to just allowing the information to be there. So … there is adding on of information in the equivalent of a WIKI without quality control up to a certain point.
KH	Who would ultimately make the decision? I think it is useful to have these different eyes looking at it, because … as I said before, how do I, how can I really interpret law enforcement data? How do they interpret health data? If I have them in the room, they can tell me how they interpret their own data. I can tell them

	how I interpret what I would consider … the area that we have expertise in … but somebody at the fusion center has to say ultimately, this is the path, the algorithm that we are following. It is just like when we have a suspicious substance it is in the field … do we have the people who are trained there and the expertise to make the decision about is this a credible threat? Is there law enforcement there? Is there public health there? And, is the HAZMAT Team there? I really think you need all three of those people there to make a decision locally whether this is a credible threat. Because at the State Health Department, I can't tell you whether something that happens four hours away is a credible threat or not.
KH	The question [is] about who makes this decision here, about is there action necessary or versus is there not any action and which pathway that you follow. Because somebody has got to be in charge. And, a lot of times … it is not really an incident yet, so … we are just talking about surveillance, there is not an Incident Commander.
BB	There needs to be a decision and there needs to be a decision to produce a product, periodically and put it in the system, so that the system is ready to receive the product and understand the context the product has been developed in.
JD	And with all those recommended actions ... it would almost seem that if you move the health threat alert, health threat notices, health threat advisories up to where assessment review is, that you could have -- at some point, when you pass those on, especially ones that require action, it [should be] somewhere in there, … I liked that you're recommending preventative actions somewhere and I don't see that on this chart …But it may be out of the fusion realm too. It may be out in the intelligence realm.
JD	Before it goes to government executives, health care sector and first responders, is there a point that it goes into a process that it assesses the criminality portion? … I mean, I see we have national threat intelligence. But it almost seems like we may be missing something there.
JD	You have to be aggressive in your feedback collection too. I mean, the Wiki can't be responsible for the process. Somebody has got to be responsible for managing it … And the Wiki could be the tool. But somebody has got to manage the Wiki and in some ways, even sort the right winger out of it or left winger out of it and say, "Okay, this is an opposing view." And that same person should be responsible for chasing feedback.
PRODUCTS	
BB	Well that is, if this system is effective, it has to continually produce products. Right after 911, the original Office of Public Safety, before it became Homeland Security in the state was excellent. They put out some very good threat assessment information for healthcare providers and EMS and a lot of it, some of it was things that there was no new threat information on them but it was just good information that they needed to keep in the back of their mind … we were posting homeland security notices, particularly to hospitals, lesser to local health departments, mostly to hospitals, and we were putting out one every 60 to 90 days.

BB	in New York we divide the health sector into healthcare system and public health system. Often the alerts have relevance for both of them. Sometimes they are only relevant for one or the other. For instance, when we had the clandestine surveillance of the hospitals going on. Guys coming in as JCAHO, didn't have any credentials, that really didn't have much applicability to the public health system, but it had a great deal to do with our healthcare system.
DG	I think that first thing is making sure is the ability to develop the product doesn't drive the product. It has to be a useable product. So, just for me to put out a weekly report that does absolutely nothing, looks great literally on paper, but it doesn't solve any of the issues… and some ways when we developed our software, we were able to drive into the software development and the program manager said wait a second we need the user requirements. So I think the core issue for the Executive Summary is what are the user requirements that have us putting this out? Does it even need to be out? Then once it is put out, I think the question is, who does it get disseminated to and you sort of hope that when you develop the user requirements that helps out. I think the third aspect of it is, and this is one of the things that is always an umbrella over everything that we always forget, is the public information aspect of it. So, the question is now that you have got the information, number one, how do you get the information out if appropriate, but number two, how do you protect the information from getting out if it is inappropriate for it to get out, especially if you have a wide spread users group. So it is not only the information and ability to have it, it is the ability to control the flow of it.
EM	I saw intelligence here although national threat is one thing, but there is also street intel[ligence]. And accommodating all of that but intel]ligence] is one of the feeds. And your end product, I saw when you came to decision here was truly this knowledge factor. And if while we are here, there is no action necessary, [this is] what we are finding and learning, for example, with food and drug administration and melamine and Chinese products. New reports this morning, Chinese keep pulling products, and etc. There is a level in here where there may be no action necessary, there is a very important part of continue to monitor
EM	One of the things to the Intel[ligence] community, actually to any of the communities, we go after very vigorously is the tear line. Because we want tear line products. We want to strip method/sources off products. We will see something and say, give us tear line on that. So, then you can have things at a much higher level classification. You get the gist of it or the actual essence of it checking with the Intel[ligence] community about how they are distributing it, but then getting our permission for us to go ahead and reference it … we really need to get tear line more and more.
NN	Right now … some of the organizations do, so CDC as reports that go out, EPI-X, and through those resources, the ATSCR, FDA, NIH have reports that go out, FDA has a lot that goes out through biological devices and for medical devices. Our immediate office does produce products regarding the situation reports and GIS products in relation to incident specific response and that information is shared, but we don't current have a standard daily report.

NN	There is a legislation or policy being promulgated in the Intelligence community right now that before any report can be released classified, it must be released UNCLASSIFIED and FOR OFFICIAL USE ONLY first before the classified version is allowed to be release. And help to ensure that we are getting information out to the user. So, I think as long as that philosophy is being maintained. I think there is a value added to getting that out there. … I definitely see the value of a health threat assessment and I think a lot of people in the sector, once they realize what it is ... And, the only other concern I can think of is … the health care sector is so diverse. You know there is medical treatment as one component or healthcare delivery systems, but there is this entire aspect in the private sector of medical distribution, materials management, so and so forth, but I think also would see a value added to this and knowing how should they deal with their supply chain and what production should they increase and decrease … how do we make the product in a way that is useable to all of them. It may be a matter of creating different products or it may be a matter of tailoring some of the data, but, I think a lot of times we focus on health care delivery systems and we ignore this entire other aspect of healthcare that without them the delivery would never occur.
NN	I think the key thing of sharing of health related situations is that it needs to be shared. So, I think there is a lot of analysis of health information in various domains in the Federal Government within DHS, outside of DHS, I think there is significant amount of importance in getting some consistent analysis done and that the product actually make it out to the end user. The generation of products, regardless of classification that sits within …that created it is essentially useless. So, making sure it covers a sector and it is diverse and that it goes out there.
EM	Because our mission focus is early queuing and situational awareness, it goes to both the First Responders and the general public. The intent of what we are trying to do is that what we find is that 98% of our data is not only UNCLASSIFIED, but is often times derived from the press and so, there has been a great focus and effort on what is in the open source world, the Intelligence Community even in the last five or six years has really put a tremendous effort into open source … a very slim portion of classified data.
COLLABORATION / TECHNOLOGY / PRODUCT	
BB	We produce a document called New York State's policy on how to evaluate suspicious substance and packages with threats. It is an FBI, State Police, Homeland Security Office of Fire Prevention Control document … I send it out to these guys and … they all gave me different comments ... not ones that I could reconcile … So, I was doing the Wiki work and … finally just brought them into the room and said come on guys … here is a draft. Everything that could be reconciled has been reconciled. Here are the comments that we couldn't reconcile, let's have it out. And we did and we ended up getting the document out and it was very successful document.
EM	The Intelligence Community using the JWICS architecture puts out TS SCI. So we have vehicles at all levels of classification to get things out. Which I think you know is important to have – that there are different vehicles. One of the things we

	do in the UNCLASS[IFIED] products, if we have something that is referring to classified data, is you put a tag line, and those that can, those that have the tag line say that is going to be SECRET, that is going to be on HSDN.
JD	I like the concept of Wiki's. I like using them. I also like them in the intelligence community. I guess the question I have here would be how would you … in what context would you be using that? Would that be an analyst using it? Would it be the members of the community?
REAL TIME	
CD	In the context of a preplanned event and/or an emergency situation resulting in data collection, the data comes primarily from, or will come from hospitals emergency department registration process. Presently the system that is populated on the HIS requires that the data for each disaster patient is hand registered on a set template which is found on the coalition's web page under a list category, however, it is anticipated by Spring of '09 we will have a much more sophisticated and more immediate collection system at hand through what we call the ED connectivity project that is going on now. That project involves taking a platform, in our case it is anticipated to be the Microsoft Amalgo Program and dropping it in over seven participating hospitals IT infrastructure to parse out select patient data that is pertaining only to general registration. It is not collecting at present lab results, X-ray results, etc. It is just parsing out name, date of birth, and admitting condition. The value of the new system is one where it doesn't require any extra work. It is real time data and will be able to be seen by not only the contributing facility but also in a disaster situation which we would classify as break the glass in its nature, we would have that data released to the other contributing hospitals as well as the DC Department of Health as well as the DC Department of Human Services. The two agencies that have the lead responsibility for family reunification.
DG	I guess you almost have to take a step back from the manifestations of what you see and what caused those manifestations and so the question [is] … what feeds do we get that allow us to come up with what we are displaying that fall in the realm of medical intelligence and I do think we get feeds from the FBI, so we get the traditional intelligence. We get feeds from our first responders calls and part of our system is a system in which we have nodes of command centers that tend to be medical command centers, that tend to be co-located with EMS Services, EMS dispatch. So consequently, the raw data of a 911 call usually makes its way into our system almost real time … The other part is the communicable disease surveillance, which at least for the State of New Jersey, is not a pure connect. There is a time delay and sometimes an organizational separation that does, that has me hesitate in saying that is always a real time feed. Other information is just random calls that we will get … we are first responders for white powder incidents, so we would respond to those incidents which provide us raw data. And then we get the standard what the FEDS will send to us and other partners send to us which they feel are necessary to spread. Also, we have inter-agency working groups that not necessarily on a real time basis, but close enough to being useable provide us information that we can feed.

KH	I think the bigger question is, [is] it collected in the real time situations so that we can really have real situational awareness? How timely is the data collected? Because three are many different health data sources that come into our central office there at the State.
KH	We have an internal kind of a direct line to many different agencies that are within what we call our cabinet in state health. So, that includes mental health, and mental retardation department. We also have what we call DCBS, which is our Department of Community Based Services and we are in the cabinet as MEDICAID. So, we can actually get data, although it is not that easy, but for instance within the last six months we now have access to the MEDICAID … Data Warehouse, so we are able to do queries on their data, so we can get health data. But again, it is not real time.
WR	A lot of what we rely on now are those systems that we have, like a health alert advisory network. But, what the Director wants to bring to the table, I guess 24/7 monitoring of acute and chronic diseases for example and being able to respond. You know have predictive and preventive measures in place.
POLICY	
DG	For example, our software model, each individual has a degree of access when they are given access to the system. Which allows them to see or not see different components. Now the decision as to what access to give them, there are some generalized policies but there is a lot of the seat of the pants part of it, So, I think that we are a mixture of policies and feel with more of a … lesser reliance on policies because we haven't fully developed then yet, not because there is not the need for it,
QUALIA	
EM	What you have is … all of this information. You have got the, agreed to, official descriptions of diseases, of those not in professional health. Maybe able to spell Tularemia, but they may not be able to tell you so what, and here they are trying to make a decision. And on the other side of your display is okay we have these facts and you start pulling in histograms, you start pulling in where are we along a time line that I can maneuver so I can see it start, grow, build, and are there models? Are there historic records? And if so it gives you the visual analytics to be able to see that whoa, whoa, this looks very similar to a case before or this doesn't look at all like the last 10 cases or the last 10 events. What it is going on here? And it is the intent to get at that.

LIST OF REFERENCES

28 Code of Federal Regulations (CFR). Part 23, Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). Retrieved November 30, 2008, from http://www.iir.com/28cfr/guideline.htm

Abbot, E. B., & Hetzel, O. J. (2005). *A legal guide to homeland security and emergency management for state and local governments*. Chicago: American Bar Association.

Ackerman, G. A., & Kevin, S. M. (2006). *Bioterrorism and threat assessment.* Stockholm, Sweden: Weapons of Mass Destruction Commission. Retrieved March 9, 2008, from http://www.wmdcommission.org/

American heritage® dictionary of the English language (4th ed.). (2004). Houghton Mifflin Company. Retrieved December 6, 2008, from http://dictionary.reference.com/browse/synergy.

Andrus, D. C. (2007). Toward a complex adaptive intelligence community. The Wiki and the Blog. *Studies in Intelligence, 9*. Retrieved October 19, 2008, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_%20Blog_7.htm

Armed Forces Medical Intelligence Center. (2000). *Medical intelligence tutorial*, Washington, D.C.: Department of Defense.

Belden, T. G. (1977). Indicators, warning, and crisis operations. *International Studies Quarterly*, *21*, 181-198.

Boselego, J. (2005). Engineering social trust. What can communities and institutions do? *Harvard International Review*. In *International Health*, *27*. Retrieved November 30, 2008, from http://www.harvardir.org/articles/print.pohp?article=1319

Boyd, John R. (1987, August). A discourse on winning and losing. *Maxwell Air Force Base*, Alabama: Air University Library, Document No. M-U 43947. Unpublished collection of briefing slides. In Michael T. Plehn, *Control of warfare. Inside the OODA loop*, Master's thesis, School of Advanced Warpower Studies, Air University, June 2000.

Brafman, O., & Beckstrom, R. A. (2006). *The Starfish and the spider. The unstoppable power of leaderless organizations*. New York: Penguin Group.

Brueggemann, C. E. (2008, March). *Mitigating information overload: The impact of "context-based approach" to the design of tools for intelligence analysts*. Master's thesis, Monterey, CA: Naval Postgraduate School, Center for Homeland Defense and Security.

Burgess, R. L., Jr. (2008, November 1). Remarks by the Director of the Intelligence Staff, *Canadian Association for Intelligence and Security Studies*, International Conference, Ottawa, Canada. Retrieved November 9, 2008, from http://www.dni.gov/speeches/20081101_speech.pdf

Butler, J. C., Cohen, M. L., Friedman, C. R., Scripp, R. M. & Watz, C. G. (October 2002). Collaboration between public health and law enforcement: New paradigms and partnerships for bioterrorism planning and response. *Emerging Infectious Diseases, 8*, 1152-1156. Retrieved September 9, 2007, from http://www.cdc.gov/ncidod/EID/vol8no10/02-0400.htm

Campbell, A., Converse, P. E., Miller, W. E., & Stokes, D. E. (1980). *The American voter*. Chicago: University of Chicago Press.

Carter, D. L. (2004). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. Washington, D.C.: Department of Justice, Michigan State University, School of Criminal Justice.

Carter, D. L. (2005, June). The law enforcement intelligence function, state, local and tribal agencies. *FBI Law Enforcement Bulletin, 74*, 383-310.

Centers for Disease Control and Prevention. (2007, August). *About PHIN. PHIN requirements. Version 2.* Retrieved January 6, 2008, from http://www.cdc.gov/phin/library/documents/pdf/111759_requirements.pdf

Centers for Disease Control and Prevention. *Guidance for developing public health alerts, advisories, or updates*. Retrieved November 16, 2008, from http://www.cdc.gov/ncphi/disss/nndss/8city.htm.

Central Intelligence Agency. (2001). *Factbook on intelligence*. Washington, D.C.: George Bush Center for Intelligence. Retrieved October 25, 2008, from http://fas.org/irp/cia/product/facttell/index.html

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals. In +organizational knowledge sharing. *Information and Management, 45*, 458-465. Retrieved December 6, 2008, from www.elsevier.com/locate/im

Cooper, J. R. (2005, December). *Curing analytic pathologies. Pathways to improved intelligence*. Washington, D.C.: Center for the Study of Intelligence.

Covey, S. R., & Merrill, R. R. (2006). *The speed of trust. The one thing that changes everything*. New York: Free Press.

Crosbie, W. L. (2008, September). *Public-private sector passenger rail intelligence and terrorism information sharing*. Master's thesis, Monterey, CA: Naval Postgraduate School, Center for Homeland Defense and Security.

Cross, R., & Parker, A. (2003). *The hidden power of social networks. Understanding how work really gets done in organizations*. Boston: Harvard Business School Press.

Curts, R. J., & Campbell, D. E. (2001). *Avoiding information overload through the understanding of OODA loops, A cognitive hierarchy and object-oriented analysis and design*. 6th International Command and Control Research and Technology Symposia, Track 4. Retrieved October 26, 2008, from http://www.dodccrp.org/events/6th_ICCRTS/Tracks/Papers/Track4/018_tr4.pdf

Danforth, M. (2006, September). *Models for threat assessment in networks*. Doctoral dissertation, Davis, California: University of California – Davis, Computer Science Department.

Davenport, T. (1997). Ten principles of knowledge management and four case studies. *Knowledge and Process Management*, *4*, 187-208.

Defense Intelligence Agency. (2008, July 2). *U.S. dedicates national medical for intelligence center; pentagon facility expands into national mission*. Washington: D.C. Retrieved November 16, 2008, from http://www.dia.mil/publicaffairs/Press/trans02.pdf

DeFraites, R. F. (2007). United States Army, Gaining experience with military medical situational awareness and geographic information systems in a simulated influenza epidemic. *Military Medicine*, *172*, 1071-1076.

Department of Homeland Security. (2005). *Interim national preparedness goal. Homeland Security Presidential Directive 8*. Washington, D.C.: Department of Homeland Security.

Department of Homeland Security. (2007). *Information gathering and recognition of indicators and warnings, exercise evaluation guide*. Washington, D.C. Retrieved December 29, 2007, from https://hseep.dhs.gov/pages/1002_EEGLi.aspx

Department of Homeland Security. (2007). *Target capabilities list*. Washington, D.C.: Department of Homeland Security.

Department of Homeland Security (n.d.). State and Local Fusion Centers. Retrieved September 18, 2008, from http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm

Department of Justice. (2006). *Fusion center guidelines. Developing and sharing information and intelligence in a new era. Guidelines for establishing and operating fusion centers at the local, state and federal levels. Law Enforcement Intelligence, Public Safety, and the Private Sector*. Washington, D.C.: Department of Homeland Security.

Department of the Army. Fort Detrick. (2008, November). Retrieved December 6, 2008, from http://www.afmic.detrick.army.mil/

Devon & Cornwall Constabulary Glossary. (2008). Retrieved December 12, 2007, from http://www.devon-cornwall.police.uk/v3/help/glossary.htm#s

District of Columbia. Reportable diseases in the District of Columbia. Retrieved November 16, 2008, from http://app.doh.dc.gov/services/administration_offices/phsa/bedc/reportable_diseases.shtm

Federal Bureau of Investigation. (2008, October 14). Domestic terrorists' intent and capability to use chemical, biological, radiological, and nuclear weapons. *Joint Special Assessment, Federal Bureau of Investigation Intelligence Assessment*. Washington, D.C.: Federal Bureau of Investigation Weapons of Mass Destruction Directorate, Counterterrorism Division, and Department of Homeland Security, Office of Intelligence and Analysis.

Fein, R.A., Vossekuil, B., Pollack, W. S., Borum, R., Modzeleski, W., & Reddy, M. (2002, May). *A guide to managing threatening situations and to creating safe school climates*. Washington, D.C.: U.S. Secret Service and Department of Education.

Fisher, J., Gronvall, J., Hate, A., Bornstein, R., Greenland, A., Ravishankar, A., & Roman, P. (2008, September). *New information and intelligence needs in the 21st century threat environment*. Washington, D.C.: Henry L. Stimson Center, Report No. 70.

Garst, R. D., & Gross, M. L. (2003). Characteristics of successful intelligence analysts. In R. G. Swenson, R. G., (Ed.), *Bringing intelligence about. Practitioners reflect on best practices* (pp. 105-126). (U.S. Army, Joint Military College, Defense Intelligence Agency, Center for Strategic Intelligence Research Publication No. D 5.202: IN 8/6). Washington, D.C.: Government Printing Office.

Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world*. Cambridge, UK: Polity Press.

Gladwell, M. (2002). *The tipping point: How little things make a big difference*. New York: Little, Brown and Company.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* New Brunswick: Aldine Transaction.

Government Accounting Office. (2006). Critical infrastructure protection. Progress coordinating government and private sector efforts varies by sector's characteristics, GAO 07-39. Washington, D.C.: Government Accounting Office.

Hansen, M. T., & Nohria, N. (2006, January). How to build collaborative advantage. *MIT Sloan Management Review*, 464, A special monograph for distribution at the World Economic Forum, Davos, Switzerland.

Horgan, T., & Tienson, J. (2002). The intentionality of phenomenology and the phenomenology of intentionality. In D. J. Chalmers (Ed.), *Philosophy of Mind* (pp. 520-533). New York: Oxford University Press.

Howes, N., & Quinn, R. (1978, March). Implementing change: From research to a prescriptive framework. *Group and Organizational Studies*, *3*, 71-84.

Jackson, F. (1982, April). Epiphenomenal qualia, *The Philosophical Quarterly*, *32*, 127-136.

Johnson, L. K., & Wirtz, J. J. (2008). *Intelligence and national security. The secret world of spies* (2nd Ed.). New York: Oxford University Press.

Kansas City Health Department. (2005, July). Community health assessment 2005, Kansas City, Missouri. Kansas City, Missouri: Kansas City Health Department.

Kentucky.gov (2008). Kentucky reportable disease. Retrieved November 16, 2008, from http://chfs.ky.gov/NR/rdonlyres/FC15DA59-4698-4CFC-919C-6E58AAD7AE45/0/KentuckyReportableForm2003.pdf

Kim, W. C., & Mauborgne, R. (2005). *Blue ocean strategy*. Boston: Harvard Business School Press.

Kleinbaum, A. M., & Tushman, M. (2008, July-August). Managing corporate social networks. *Harvard Business Review*, Reprint F0807J.

Lewis, M. D., Pavlin, J. A., Mansfield, J. L., O'Brien, S., Boomsma, L. G., Elbert, Y., & Kelley, P. W. (2002). Disease outbreak detection system using syndromic data in the greater Washington, D.C. area. *American Journal of Preventive Medicine, 23*, 180-186. Retrieved December 6, 2008, from http://www.sciencedirect.com/science/article/B6VHT-46T9D7X-6/2/e83b7313402784e10f2cef433eb643a4

Lombardo, J. S. (2003). The ESSENCE II disease surveillance test bed for the national capital area. *Johns Hopkins Technical Digest, 24*, 327-324. Retrieved December 6, 2008, from http://www.jhuapl.edu/techdigest/td2404/Lombardo.pdf

Lorenz, E. (1972). *Predictability: Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?* American Association for the Advancement of Science Conference, Washington, D.C. Retrieved November 1, 2008, from http://crossgroup.caltech.edu/chaos_new/lorenz.html

Louisville Metro Department of Health. (2006). *Health status assessment report 2006.* Louisville, Kentucky: Department of Health.

Lowenthal, M. M. (2006). *Intelligence. From secrets to policy* (3rd ed.). Washington, D.C.: Congressional Quarterly Press.

Lurie, N., Gresenz, C. R., Blanchard, J. C., Ruder, T., Chandra, A., Ghosh-Dastidar, et al. (2008, January). *Assessing health and health care in the District of Columbia*, Washington, D.C.: RAND.

Masood, A. (2008. November 15). Reuters photograph. *The Washington Post* (Northern Virginia, Ed.) p. A9.

Masse, T., O'Neil, S., & Rollins, J. (2007, July 6). Fusion centers: issues and options for Congress. Washington, D.C.: Congressional Research Service. (Order Code RL34070).

McConnell, J. M. (n.d.). *Vision 2015. A globally networked and integrated intelligence enterprise*. Introductory Letter. Washington, D.C.: Office of the Director, National Intelligence.

McConnell, J. M. (2008, February 27). Statement made to the Senate Armed Services Committee, on Annual Threat Assessment of the Director of the National Intelligence, 110th Cong., 1st sess. Retrieved March 9, 2008, from http://www.dni.gov/testimonies/20080227_testimony.pdf

McCoy, D., Pezzini, M., Natis, Y., Schulte, R., Thompson, J., & Lheureux, B., et al. (2003, May 30). Hype cycle for application integration and platform middleware, *Strategic Analysis Report*, Gartner, 7. Retrieved November 16, 2008, from http://dhs.wisconsin.gov/aboutdhs/ITcollaboration/HypeCycleForAppIntegration.pdf

Mingers, J. (2001, September). Combining IS research methods: Towards a pluralist methodology. *Information Systems Research*, *12*, 240-259.

Moore, D. T., & Krizan, L. (2003). Core competencies for intelligence analysis at the National Security Agency. In R. G. Swenson, (Ed.), *Bringing intelligence about. Practitioners reflect on best practices* (pp. 95-104). U.S. Army, Joint Military College, Defense Intelligence Agency, Center for Strategic Intelligence Research Publication No. D 5.202: IN 8/6. Washington, D.C.: Government Printing Office.

Morrissey, J. (2007, March). *Strategies for integration of medical and health representation within law enforcement intelligence fusion centers*. Master's thesis, Monterey, CA: Naval Postgraduate School, Center for Homeland Defense and Security.

Natarajan, N. (2007, September). *National imperative to establish a domestic medical intelligence center*. Master's thesis, Monterey, CA: Naval Postgraduate School, Center for Homeland Defense and Security.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 commission report*. 1st ed. New York: W.W. Norton & Company.

National Governor's Association. (2007, December). *2007 State homeland security director's survey*. Washington, D.C.: National Governor's Association. Retrieved October 26, 2008, from http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=36c8c1e0edde6110VgnVCM1000001a01010aRCRD

Office of The Director of National Intelligence. (2008, November 5). *TIME rates A-Space among year's best 50 inventions*, News Room. Retrieved November 11, 2008, from http://www.odni.gov/odni_2.htm

Oliver-Hoyo, M., & Allen, D. (2006, January/February). The use of triangulation methods in qualitative educational research. *Journal of College Science Teaching*, 42-47.

Polzner, Jeffrey T. (2008, July-August). Making diverse teams click. *Harvard Business Review*, 20-21. Reprint F0807C.

Richards, E. P. (2002, October). Collaboration between public health and law enforcement: The constitutional challenge. *Emerging Infectious Diseases*, *8* (n.p.). Retrieved September 9, 2007, from http://www.cdc.gov/ncidod/EID/vol8no10/02-0465.htm

Rolka, H., O'Connor, J. C., & Walker, D. (In Press). Public health information fusion for situation awareness. Biosurveillance and biosecurity: Systems and Algorithms, Biosecurity 2008 Proceedings. *Lecture Notes in Computer Science*. New York: Springer.

Runge, J. W. (2008, April 21). UASI Keynote Address by Assistant Secretary for Health Affairs, Department of Homeland Security. Retrieved September 18, 2008, from http://www.dhs.gov/xnews/speeches/sp_1211999308849.shtm

Sagan, C. (1996). *The demon haunted world. Science as a candle in the dark*. New York: Ballantine Books.

Samarati, P., & Sweeney, L. (Unpublished). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Retrieved February 18, 2008, from http://citeseer.ist.psu.edu/samarati98protecting.html

Schoenberg, R. (2001). Knowledge transfer and resource sharing as value creation mechanisms in inbound continental European acquisitions. *Journal of Euromarketing*, *10*, 99-114.

Smith, H., & McKeen, J. D. (2004). Developments in practice XII: Knowledge-enabling business processes. *Communications of the Association for Information Systems, 13*, 25-38. Queen's School of Business, Queen's University. In Gartner Group (2004). D. McCoy, M. Pezzini, Y. Natis, R. Schulte, J. Thompson, B. Lheureux, J. Sinur, and F. Kenney, (Ed.), Hype cycle for application integration and platform middleware, *Strategic Analysis Report*, May 30, 2003, Retrieved November 16, 2008, from http://dhs.wisconsin.gov/aboutdhs/ITcollaboration/HypeCycleForAppIntegration.pdf

Strawson, G. (1994). *Mental reality*. Cambridge, MA: Massachusetts Institute of Technology (MIT Press).

Thomas, G. F., Hocevar, S., & Jansen, E. (2008, September 25). *A diagnostic approach to building collaborative capacity in an interagency context*. Naval Postgraduate School Rep. No. NPS-GSBPP-06-013. Monterey, CA: Naval Postgraduate School, Acquisition Research Sponsored Report Series.

Transportation Security Administration (2004, August 17). *Security threat assessment for aircraft operators and heliport operators and their employees that conduct air tour operations in New York City*. Washington, D.C.: Department of Homeland Security.

Tye, M. (2002). Visual qualia and visual content revisited. In D. J. Chalmers (Ed.), *Philosophy of Mind* (pp. 447-456). New York: Oxford University Press.

Tye, M. (2008, Fall). Qualia. *The Stanford encyclopedia of philosophy*. E. N. Zalta (Ed.). Retrieved October 26, 2008, from http://plato.stanford.edu/archives/fall2008/entries/qualia/

Von Kortzfleisch, H. F.O., Margel, I., & Proll, C. (2007). Potentials of social networks for knowledge management with regard to the development of stable competences and dynamic capabilities – conceptualization and case study results. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences - 2007 (HICSS'07)*. U.S.: IEEE, The Computer Society.

Warrick, J., & Tate, J. (2008, November 15). Experts see security risks in downturn. global financial crisis may fuel instability and weaken U.S. defenses. *The Washington Post* (Northern Virginia Ed.) pp. A1, A9.

Wasko, M. M., & Faraj, S. (2005, March). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, *29*, 35-57.

Zhuge, H. (2002). A knowledge flow model for peer-to-peer team knowledge sharing and management. *Expert Systems with Applications*, *23*, 23-30.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Neil Troppman
   Bureau of Alcohol, Tobacco, Firearms and Explosives
   Martinsburg, West Virginia

4. Pierre N. D. Vigilance, M.D.
   Department of Health
   District of Columbia Government
   Washington, D.C.

5. Sarah Canzano
   Webster, New York

6. Lisa Schwenk
   Jefferson City, Missouri

7. Scott Pickett
   U.S. Federal Air Marshal Service
   Transportation Security Administration
   Brooklyn Heights, Ohio